THE YALE LAW JOURNAL

JONATHAN MAYER

Government Hacking

ABSTRACT. The United States government hacks computer systems for law enforcement purposes. As encryption and anonymization tools become more prevalent, the government will foreseeably increase its resort to malware.

Law enforcement hacking poses novel puzzles for criminal procedure. Courts are just beginning to piece through the doctrine, and scholarship is scant. This Article provides the first comprehensive examination of how federal law regulates government malware.

Part I of the Article considers whether the Fourth Amendment regulates law enforcement hacking. This issue has sharply divided district courts because, unlike a conventional computer search, hacking usually does not involve physical contact with a suspect's property. The Article provides a technical framework for analyzing government malware, then argues that a faithful application of Fourth Amendment principles compels the conclusion that government hacking is inherently a search.

Part II analyzes the positive law that governs law enforcement hacking, answering fundamental criminal procedure questions about initiating a search, establishing probable cause and particularity, venue, search duration, and notice. A review of unsealed court filings demonstrates that the government has a spotty compliance record with these procedural requirements. The Article also argues for reinvigorating super-warrant procedures and applying them to law enforcement hacking.

Finally, Part III uses government malware to illuminate longstanding scholarly debates about Fourth Amendment law and the structure of surveillance regulation. Law enforcement hacking sheds new light on the interbranch dynamics of surveillance, equilibrium adjustment theories for calibrating Fourth Amendment law, and the interplay between statutory and constitutional privacy protections.

AUTHOR. Cyber Initiative Fellow, Stanford University; Assistant Professor of Computer Science and Public Affairs, Princeton University (effective March 2018); J.D., Stanford Law School; Ph.D. candidate, Stanford University Department of Computer Science. The author currently serves as a Legislative Fellow in the Office of United States Senator Kamala D. Harris. All views are solely the author's own and do not reflect the position of the United States government. This work draws upon conversations at the Federal Judicial Center Fourth Circuit Workshop, Federal Judicial Center Sixth Circuit Workshop, Federal Judicial Center Ninth Circuit Mid-Winter Workshop, Federal Judicial Center Workshop for United States Magistrate Judges, the Privacy Law Scholars Conference, and the Rethinking Privacy and Surveillance in the Digital Age event at Harvard Law School. The project benefits from the wisdom and feedback of countless colleagues, including Julia Angwin, Kevin Bankston, Dan Boneh, Ryan Calo, Cindy Cohn, Laura Donohue, Hanni Fakhoury, Nick Feamster, Ed Felten, Laura Fong, Jennifer Granick, James Grimmelmann, Marcia Hofmann, Orin Kerr, Mark Lemley, Whitney Merrill, John Mitchell, Ellen Nakashima, Paul Ohm, Kurt Opsahl, David Pozen, Chris Riley, Barbara van Schewick, Michael Shih, David Sklansky, Peter Swire, Elisabeth Theodore, Lee Tien, George Triantis, and Tyce Walters. The editors of the *Yale Law Journal*, led by Jeremy Aron-Dine, provided invaluable recommendations on the Article's substance and organization. The author is especially grateful to the federal judges, attorneys, and law enforcement officers who informed this Article's discussion of the law, policy, and technology issues associated with government hacking.

ARTICLE CONTENTS

INTRODUCTION 574

I. IS LAW ENFORCEMENT HACKING A FOURTH AMENDMENT "SEARCH"? 581

A. The Technical Architecture of Government Malware 583

1. Delivery 583
2. Exploitation 586
3. Execution 588
4. Reporting 589

B. Conventional Methods for Obtaining Electronic Evidence and Corresponding Perspectives on Fourth Amendment Privacy 590

1. Physical Access to an Electronic Device and the Device-Centric Perspective 590
2. Remote Access to Information via a Third Party and the Data-Centric Perspective 592

C. Obtaining Electronic Evidence by Hacking 594

1. The Easy Scenarios: Physical Access or Content 594
2. The Hard Scenario: Remote Access to Metadata 596

a. A Plausible Position: No Fourth Amendment Protection 596

i. Mobile Phone Location Tracking 600
ii. ISP Surveillance 601
iii. Mobile Phone Serial Numbers 603
iv. Payment Card Magnetic Stripes 604
v. Placing Telephone Calls 604

b. A Better Position: The Fourth Amendment Protects Logical Integrity 609

i. *Katz v. United States* 609
ii. *Riley v. California* 609
iii. Cloud Service Searches and United States v. Warshak 610
iv. The Consent-Based Limiting Principle for Constitutional Information Privacy 611
v. Policy Considerations 613

II. RULES FOR MALWARE 614
A. Initiating a Search 615
B. Probable Cause and Particularity 620
C. Venue 625
D. Search Duration 628
E. Notice 633
F. Super-Warrant Requirements 638
G. Policy Arguments in Favor of Always Requiring a Super-Warrant 641

III. LESSONS FOR FOURTH AMENDMENT THEORY 644
A. The Interbranch Dynamics of Surveillance Regulation 646
1. Competing Judicial and Scholarly Perspectives 646
2. The Executive Branch Can Self-Regulate Privacy Practices Through Interagency Processes 649
3. Executive Branch Privacy Protections Can Exceed Judicial and Legislative Protections 650
4. Courts Exhibit Regulatory Capture in Law Enforcement Surveillance Litigation 651
5. Courts Are Capable of Understanding Novel Surveillance Technology 652
6. Congress Is Not Taking Action 653
B. Equilibrium-Adjustment and Substitution Theories Are Indeterminate and Risk Misleading Courts 654
C. Positive Law Is a Factual Guide, but Not Necessarily a Legal Guide, for Constitutional Articulation 657

CONCLUSION 659

APPENDIX 661

"Hacking devices, . . . of course we do it . . . ."
– James Baker, General Counsel, Federal Bureau of Investigation[1]

INTRODUCTION

Timberline High School was gripped by panic.[2] In the span of just over a week, the suburban Washington school had received *nine* anonymous bomb threats, prompting repeated evacuations and police sweeps.[3] The perpetrator taunted academic administrators with a slew of emails, and he spooked students from a threatening social network account.[4] He also knocked campus computer systems offline.[5]

Local police and the county sheriff were stumped. Officers had obtained information about the perpetrator's network access and accounts, but the traffic was routed through a pair of computers in Italy and the Czech Republic.[6] After exhausting their conventional investigative tools, the local authorities called in the FBI.[7]

1. Jenna McLaughlin, *FBI's Secret Surveillance Tech Budget Is 'Hundreds of Millions,'* INTERCEPT (June 25, 2016, 10:49 AM), http://theintercept.com/2016/06/25/fbis-secret-surveillance-tech-budget-is-hundreds-of-millions [http://perma.cc/76J4-GFHD] (quoting Baker).

2. *See* Raphael Satter, *How a School Bomb-Scare Case Sparked a Media vs. FBI Fight*, ASSOCIATED PRESS (Mar. 18, 2017), http://www.ap.org/ap-in-the-news/2017/how-a-school-bomb-scare-case-sparked-a-media-vs.-fbi-fight [http://perma.cc/5LZP-KBZ4]. *See generally* Cyber Div., Fed. Bureau of Investigation, *Situation Action Background: Timberline School District* (Oct. 29, 2014), *in* 2 REPORTERS COMM. FOR FREEDOM OF THE PRESS, FBI DOCUMENT PRODUCTION at RCFP-44, https://www.rcfp.org/sites/default/files/litigation/rcfpapfoia_2016-02-26_fbi_document_production_part_2_of_5.pdf [http://perma.cc/SF87-W6VM] (providing background on the bomb threat and the FBI's decision to impersonate a member of the media).

3. *Lacey 10th-Grader Arrested in Threats To Bomb School*, SEATTLE TIMES (June 14, 2007, 4:01 PM), http://www.seattletimes.com/seattle-news/lacey-10th-grader-arrested-in-threats-to-bomb-school [http://perma.cc/4H35-N9KH].

4. *See* Application and Affidavit for Search Warrant at 6-10, *In re* Search of Any Comput. Accessing Elec. Message(s) Directed to Adm'r(s) of MySpace Account "Timberlinebombinfo" and Opening Messages Delivered to that Account by the Gov't, No. MJ07-5114 (W.D. Wash. June 12, 2007) (on file with author).

5. *See* Office of the Inspector Gen., *A Review of the FBI's Impersonation of a Journalist in a Criminal Investigation*, U.S. DEP'T JUST. 9 (Sept. 2016), https://oig.justice.gov/reports/2016/01607.pdf [http://perma.cc/Z3RN-WCVL].

6. *Id.* at 10.

7. *Id.*

One week later, FBI agents penned a fake Associated Press article about the incident.[8] They drafted the title and content to pander to the hoaxer's ego, portraying him as a tech-savvy prodigy who had outwitted the local authorities.[9] Then, they sent a link to the hoaxer's social network account, hoping he would click.[10]

He took the bait. When he loaded the news story, he unwittingly installed FBI malware—which surreptitiously circumvented security protections in his web browser, bypassed his proxy connection through Italy, and reported his Internet Protocol (IP) address to an FBI server in Virginia.[11] An FBI agent forwarded the IP address to local police, who determined it was associated with a Comcast broadband subscriber. They issued an exigent request to Comcast, which quickly responded with an account name and address.[12]

Hours later, just after midnight, a SWAT team raided the residence.[13] They discovered a teenage student who attended Timberline High.[14] He immediately admitted culpability.[15]

* * *

Law enforcement malware is not new.[16] The earliest reported case is from 2001, when FBI agents snuck into a mafioso's office and installed a system for

8. *Id.* at 14.
9. *Id.* at 15-16.
10. *Id.*
11. Application and Affidavit for Search Warrant, *supra* note 4, at 13; Cyber Div., *supra* note 2.
12. Cyber Div., *supra* note 2, at RCFP-46.
13. *Id.*
14. Office of the Inspector Gen., *supra* note 5, at 16.
15. *Id.*
16. Referring to these practices as "malware" is a source of some controversy. *Compare* United States v. Arterbury, No. 15-CR-182-JHP, 2016 BL 133752, at *6 (N.D. Okla. Apr. 25, 2016) (referring to FBI software as "malware"), *with* United States v. Matish, 193 F. Supp. 3d 585, 601-02 (E.D. Va. 2016) (objecting to characterization of a government program as "malware"). I use the term "malware" throughout this Article because, in the field of computer security, it is the common term for software that subverts a user's device. The term is not intended as a criticism of government hacking. On the contrary, my view is that hacking can be a legitimate and effective law enforcement technique. I also use the term to promote consistency and avoid ambiguity. Government documents have referred to hacking with a wide variety of terms, including Network Investigative Technique (NIT), Computer and Internet Protocol Address Verifier (CIPAV), Internet Protocol Address Verifier (IPAV), Remote Access Search and Surveillance (RASS), Remote Computer Search, Remote Search, Web Bug, Sniffer, Computer Tracer, Internet Tracer, and Remote Computer Trace.

recording keystrokes.[17] What *is* new is how often federal law enforcement is deploying malware.[18]

Over the past decade, privacy and security technologies have become much easier to use. Individuals and businesses are rapidly adopting technical protections, especially in the wake of the Edward Snowden leaks. Usage of the Tor anonymization software, for example, has roughly doubled since fall 2013.[19] Apple has made storage encryption the default for macOS and iOS devices, protects iMessage conversations with end-to-end encryption, and it is moving toward greater hardware protections for data.[20] Google has mostly made storage encryption the default for Android devices.[21] Facebook offers optional end-to-end encryption for messages on its social network and automatic end-to-end encryption for messages sent via its WhatsApp messaging app.[22]

---

17. *See* United States v. Scarfo, 180 F. Supp. 2d 572, 574 (D.N.J. 2001). The *Scarfo* opinion provides only a summary of the FBI's "Key Logger System," recognizing it as protected from disclosure under the Classified Information Procedures Act. What details are included suggest a design with both hardware and software components. Later in 2001, news reports confirmed that the FBI was developing sophisticated malware, euphemistically entitled "Magic Lantern" and the "Enhanced Carnivore Project." *See* Bob Sullivan, *FBI Software Cracks Encryption Wall*, MSNBC (Nov. 20, 2001), http://www.nbcnews.com/id/3341694/ns/technology_and_science-security/t/fbi-software-cracks-encryption-wall [http://perma.cc/Y9D5-WVUA].

18. *See* Letter from Mythili Raman, Acting Assistant Att'y Gen., U.S. Dep't of Justice, Criminal Div., to Judge Reena Raggi, Chair, Advisory Comm. on the Criminal Rules 1 (Sept. 18, 2013) (describing government hacking practices as "increasingly common situations"); *see also* Email from [Redacted] to CTCs, Re [Redacted] (Mar. 7, 2002), *in* 5 ELEC. FRONTIER FOUND., CIPAV FOIA RELEASE 1, https://www.eff.org/files/filenode/cipav/fbi_cipav-05.pdf [http://perma.cc/3BVV-G6YM] ("[W]e are seeing indications that [the Internet Protocol Address Verifier (IPAV)] technique is being used needlessly by some agencies . . . .").

19. *See Users [Start Date: 2013-01-01, End Date: 2016-12-31, Source: All users]*, TOR PROJECT, https://metrics.torproject.org/userstats-relay-country.html?start=2013-01-01&end=2016-12-31&country=all&events=off [http://perma.cc/JNW4-LKNU]. *See generally* Roger Dingledine et al., *Tor: The Second-Generation Onion Router* (2004), http://svn.torproject.org/svn/projects/design-paper/tor-design.pdf [http://perma.cc/3QBZ-YGWW] (describing Tor).

20. Ivan Krstic, *Behind the Scenes of iOS Security*, YOUTUBE (Aug. 16, 2016), https://www.youtube.com/watch?v=BLGFriOKz6U [http://perma.cc/N8HR-GU2N].

21. *Android 7.1 Compatibility Definition Document*, GOOGLE, http://source.android.com/compatibility/android-cdd.html [http://perma.cc/Q969-WM3C] ("[T]he data storage encryption MUST be enabled by default at the time the user has completed the out-of-box setup experience.").

22. *Messenger Secret Conversations: Technical Whitepaper*, FACEBOOK 3 (July 8, 2016), http://fbnewsroomus.files.wordpress.com/2016/07/secret_conversations_whitepaper-1.pdf [http://perma.cc/3QM6-EZU4]; *WhatsApp Encryption Overview: Technical Whitepaper*, WHATSAPP 3 (July 6, 2017), http://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf [http://perma.cc/56Y9-UFW6].

These privacy and security technologies provide legitimate and important protections. But they also inhibit tried-and-true law enforcement techniques. Investigators used to be able to subpoena an Internet Service Provider (ISP) for an online suspect's identity; internet anonymization software makes that impossible. Investigators used to be able to serve a search warrant or wiretap order on a cloud service to obtain a suspect's online communications; end-to-end encryption makes that impossible. Investigators used to be able to seize a suspect's computer and smartphone and search their data contents; device encryption makes that impossible. The law enforcement community refers to this trend as "going dark," and it has sought assistance from technology firms and legislatures to reverse the trend.[23]

There is, to be sure, an ongoing and lively debate over the extent to which law enforcement agencies are actually "going dark" and how law and policy should respond if they are.[24] One aspect of the debate is indisputable: certain law enforcement techniques for electronic searches and seizures are no longer effective, and the natural substitute for those techniques is hacking.[25] If the government cannot learn a suspect's identity from his ISP, it can break into his computer and retrieve identifying information. If the government cannot obtain a suspect's communications from his cloud services, it can break into the suspect's computer, retrieve stored communications, and intercept future conversations. If the government cannot read the encrypted data stored on a suspect's devices, it can break into those devices to extract unencrypted data or the cryptographic

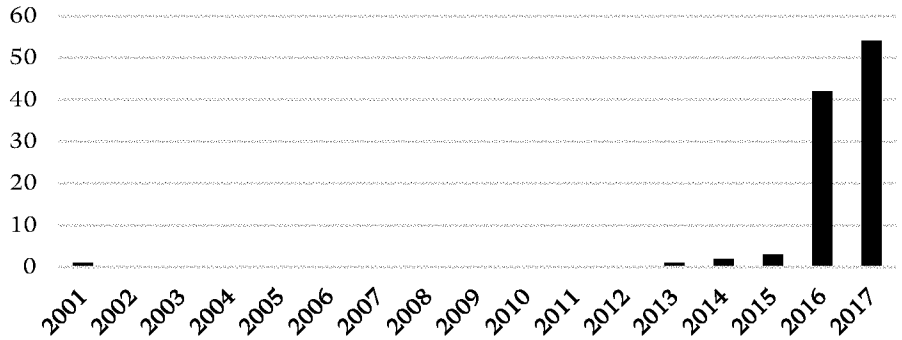
23. *See Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. 1 (2015) (joint statement of Sally Quillian Yates, Deputy Att'y Gen. of the United States, and James Comey, Director of the FBI); Majority Staff, *Going Dark, Going Forward: A Primer on the Encryption Debate*, HOUSE COMMITTEE ON HOMELAND SECURITY (June 2016), http://homeland.house.gov/wp-content/uploads/2016/07/Staff-Report-Going-Dark-Going-Forward.pdf[http://perma.cc/86AK-42QD].

24. *See* COMPUT. SCI. & TELECOMM. BD., NAT'L ACAD. OF SCIS., ENG'G & MED., EXPLORING ENCRYPTION AND POTENTIAL MECHANISMS FOR AUTHORIZED GOVERNMENT ACCESS TO PLAINTEXT (2016); Harold Abelson et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, MASS. INST. TECH. (July 7, 2015), http://dspace.mit.edu/handle/1721.1/97690 [http://perma.cc/E5NV-V74G]; Urs Gasser et al., *Don't Panic: Making Progress on the "Going Dark" Debate*, BERKMAN KLEIN CTR. FOR INTERNET & SOC'Y AT HARV. U. (Feb. 1, 2016), http://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [http://perma.cc/6LFP-TCHW].

25. An archive of FBI documents released under the Freedom of Information Act includes a diverse range of requests for hacking assistance. *See* 10 ELEC. FRONTIER FOUND., CIPAV FOIA RELEASE 1-19, https://www.eff.org/files/filenode/cipav/fbi_cipav-10.pdf [http://perma.cc/T4P6-D9VJ]; 13 ELEC. FRONTIER FOUND., CIPAV FOIA RELEASE 1-20, https://www.eff.org/files/filenode/cipav/fbi_cipav-13.pdf [http://perma.cc/DD9Z-S7CN].

material necessary for decryption. These substitution effects are not hypothetical – they are happening today. The FBI has already deployed malware to investigate a wide range of offenses, including loansharking, harassment, extortion, fraud, and child pornography. As security and privacy technology becomes more prevalent, law enforcement hacking will only become more commonplace.

FIGURE 1.
FEDERAL COURT OPINIONS ADDRESSING GOVERNMENT HACKING



The rapid rise of government malware has, surprisingly, only just begun to capture judicial attention. Through 2015, there were only a few federal opinions on the practice.[26] In 2016 and 2017, there were nearly a hundred (see Figure 1).[27] Scholarly treatment of the subject remains scattershot.[28]

26. United States v. Pierce, No. 8:13CR106, 2014 WL 5173035 (D. Neb. Oct. 14, 2014); United States v. Pierce, No. 8:13CR106, 2014 U.S. Dist. LEXIS 108171 (D. Neb. July 28, 2014) (magistrate recommendation in same prosecution); *In re* Warrant To Search a Target Comput. at Premises Unknown, 958 F. Supp. 2d 753 (S.D. Tex. 2013); United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001).

27. The data in Figure 1 reflect individually identified opinions from 2001 to 2014, *see supra* note 26, and opinions on Westlaw that match the query "network investigative technique" from 2015 to 2017.

28. Recent scholarship has emphasized jurisdictional and venue issues with law enforcement hacking. *See, e.g.*, Devin M. Adams, *The 2016 Amendments to Criminal Rule 41: National Search Warrants To Seize Cyberspace, "Particularly" Speaking*, 51 U. RICH. L. REV. 727 (2017); Susan W. Brenner, *Law, Dissonance, and Remote Computer Searches*, 14 N.C. J.L. & TECH. 43 (2012) (suggesting how to reconcile differing jurisdictional privacy standards in a remote computer search); Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075 (2017) (criticizing government hacking for intruding upon the sovereignty interests of other nations); Orin S. Kerr & Sean D. Murphy, *Government Hacking To Light the Dark Web: What Risks to International Relations and International Law?*, 70 STAN. L. REV. ONLINE 58 (2017) (responding to Ghappour); Zach Lerner, *A Warrant To Hack:*

An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure, 18 YALE J.L. & TECH. 26 (2016) (reviewing proposed revisions to the federal warrant venue rules); Brian L. Owsley, *Beware of Government Agents Bearing Trojan Horses*, 48 AKRON L. REV. 315 (2015) (reviewing five district court opinions on government hacking, primarily related to venue issues).

Several articles have raised policy concerns about technical properties of government malware. *See, e.g.*, Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1 (2014) (describing policy considerations associated with a shift from conventional wiretapping to law enforcement hacking); Benjamin Lawson, Note, *What Not to "Ware,"* 35 RUTGERS COMP. & TECH. L.J. 77 (2008) (categorizing types of government hacking); Steven M. Bellovin, Matt Blaze & Susan Landau, *Insecure Surveillance: Technical Issues with Remote Computer Searches*, COMPUTER, Mar. 2016, at 14 (describing policy considerations associated with a shift from conventional wiretapping to law enforcement hacking).

Authors have also noted how hacking is a response to growing adoption of encryption and anonymization tools. *See, e.g.*, Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, GEO. L. REV. (forthcoming 2018) (reviewing law enforcement mechanisms for defeating encryption, including hacking); Stephanie K. Pell, *You Can't Always Get What You Want: How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era?*, 17 N.C. J.L. & TECH. 599 (2016) (arguing that broader deployment of security technology will require the government to either undermine security or resort to hacking); Susan Hennessey, *The Elephant in the Room: Addressing Child Exploitation and Going Dark*, HOOVER INST. (2017), http://www.hoover.org/sites/default/files/research/docs/hennessey_webreadypdf.pdf [http://perma.cc/6J6Q-JKZK] (arguing that law enforcement hacking is a legitimate response to child exploitation and encryption and reviewing litigation associated with the Playpen investigation).

A couple articles have touched on Fourth Amendment considerations for government malware. *See, e.g.*, Susan W. Brenner, *Fourth Amendment Future*, 81 MISS. L.J. 1229 (2012) (arguing that if the government remotely retrieves files from a suspect's hard drive, it must obtain a warrant); Gus Hosein & Caroline Wilson Palow, *Modern Safeguards for Modern Surveillance*, 74 OHIO ST. L.J. 1071, 1093-97 (2013) (briefly arguing that most government malware requires a warrant); *see also* ACLU et al., *Challenging Government Hacking in Criminal Cases*, ACLU (Mar. 2007), https://www.aclu.org/sites/default/files/field_document/malware_guide_3-30-17-v2.pdf [http://perma.cc/P5UE-ASLW] (reviewing possible challenges to government hacking under the Fourth Amendment and Federal Rules of Criminal Procedure).

The opinion in *United States v. Scarfo* generated a small body of commentary. *See, e.g.*, Angela Murphy, *Cracking the Code to Privacy: How Far Can the FBI Go?*, 2002 DUKE L. & TECH. REV. 0002 (explaining the *Scarfo* case); Nathan E. Carrell, Note, *Spying on the Mob:* United States v. Scarfo—*A Constitutional Analysis*, 2002 U. ILL. J.L. TECH. & POL'Y 193 (2002) (reviewing *Scarfo* and arguing that keystroke monitoring should require a super-warrant); Neal Hartzog, Comment, *The "Magic Lantern" Revealed: A Report of the FBI's New 'Key Logging' Trojan and Analysis of Its Possible Treatment in a Dynamic Legal Landscape*, 20 J. MARSHALL J. COMPUTER & INFO. L. 287 (2002) (arguing that *Scarfo* was rightly decided); Rachel S. Martin, Note, *Watch What You Type: As the FBI Records Your Keystrokes, the Fourth Amendment Develops Carpal Tunnel Syndrome*, 40 AM. CRIM. L. REV. 1271 (2003) (arguing that keystroke monitoring should require a super-warrant).

This Article aims to begin filling the analytical void, offering guidance for courts and enriching dialogue with policymakers and scholars.[29] It also draws upon law enforcement hacking as the latest flashpoint for electronic surveillance, using the practice to illuminate and advance longstanding scholarly debates about the Fourth Amendment.

The balance of the Article is organized in three Parts. Part I begins with a motivating question of positive law: is government malware necessarily regulated by the Fourth Amendment? The Part provides a technical framework for evaluating government malware and explains how malware lands in a gap in the case law on electronic evidence. This Article respectfully submits that many courts are getting the law wrong: although about half of the lower courts that have considered the issue have concluded that law enforcement hacking does not inherently implicate constitutional privacy safeguards, the substantially better interpretation of doctrine is that government hacking is necessarily a Fourth Amendment search.

Part II answers fundamental criminal procedure questions about law enforcement hacking, including when hacking becomes a Fourth Amendment

---

The debate about law enforcement hacking is not confined to the United States. The European Union, for example, is grappling with the same issue. *See, e.g.*, MIRJA GUTHEIL ET AL., EUROPEAN PARLIAMENT DIRECTORATE-GEN. FOR INTERNAL POLICIES, LEGAL FRAMEWORKS FOR HACKING BY LAW ENFORCEMENT: IDENTIFICATION, EVALUATION AND COMPARISON OF PRACTICES (2017) (summarizing how six EU member states and three non-EU countries regulate law enforcement hacking and providing policy proposals).

29. This Article is focused exclusively on government hacking for law enforcement purposes. Hacking for national security purposes introduces further legal complications (under the Fourth Amendment and the Foreign Intelligence Surveillance Act), as well as numerous additional policy dimensions. The Article is also exclusively focused on hacking of domestic computer systems. The extraterritorial scope of the Fourth Amendment remains a subject of professional and scholarly debate. *See generally* United States v. Ulbricht, No. 14-cr-68 (KBF), 2014 U.S. Dist. LEXIS 145553, at *13-14 (S.D.N.Y. Oct. 10, 2014) (considering how the Fourth Amendment might apply to the search of a foreign server); Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326 (2015) (arguing that traditional Fourth Amendment concepts of territoriality are a poor fit for electronic data); David G. Delaney, *Widening the Aperture on Fourth Amendment Interests: A Comment on Orin Kerr's* The Fourth Amendment and the Global Internet, 68 STAN. L. REV. ONLINE 9 (2015) (similar); Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285 (2015) (summarizing territorial Fourth Amendment doctrine and applying it to international data searches).

This Article is also focused exclusively on federal hacking because the factual and legal issues are better developed for federal law enforcement. It is foreseeable that state, county, and municipal law enforcement agencies will also adopt hacking as an investigative technique. In some instances, they already have – commercial tools for breaking into smartphones, for example, are already widespread. Future work might consider the status of hacking under state law and whether certain hacking tools should be reserved for federal law enforcement.

search, who can issue hacking warrants and under what circumstances, and what notice is required to owners of hacked devices. This Article also argues for reinvigorating super-warrant procedures and applying them to government hacking, in order to channel law enforcement away from surveillance techniques that impose negative externalities.

Part III shifts to Fourth Amendment theory, using government malware as a natural experiment for reexamining three areas of scholarly discussion: interbranch dynamics in articulating surveillance regulation, recalibrating the Fourth Amendment to account for new technology, and the interplay between statutory privacy protections and constitutional privacy safeguards.

I. IS LAW ENFORCEMENT HACKING A FOURTH AMENDMENT "SEARCH"?

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[30]

Over the past century, courts have fashioned this textual command into a framework of information privacy law. The doctrinal analysis proceeds from a foundational question: does a government investigative technique constitute a

30. U.S. CONST. amend. IV.

"search"?[31] If it does, courts will scrutinize the privacy procedures associated with the tactic.[32] If it does not, judicial oversight is nonexistent.[33]

As noted earlier, about half of the district courts that have considered the issue have – surprisingly – concluded that law enforcement hacking is not necessarily a Fourth Amendment search, and that the most common configuration of government malware is exempt from ex ante judicial supervision.[34] Courts that have recognized law enforcement hacking as a search, meanwhile, have tended to offer muddled analyses and struggled to articulate how the Fourth Amendment applies to malware.[35]

This Part contributes a positive law analysis of government hacking under the Fourth Amendment. Section A begins with a technology primer, explaining

---

31. *See* William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1823, 1829 (2016) (describing the threshold inquiry in modern Fourth Amendment law); Orin Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 528-29 (2007) (same); Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1514 (2010) (same). This Article focuses exclusively on search doctrine rather than seizure doctrine, because seizures – which are grounded in personal freedom of movement and possessory interests in property – are a poor fit for electronic surveillance. *See* Brendlin v. California, 551 U.S. 249, 255 (2007) (emphasizing that seizures of persons involve "physical force or show of authority" (quoting Florida v. Bostick, 501 U.S. 429, 434 (1991))); United States v. Jacobsen, 466 U.S. 109, 113 (1984) ("A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property."). While some courts and scholars occasionally refer to forms of electronic surveillance (and especially copying data) as a species of seizure, categorization as a search is more consistent with current Fourth Amendment doctrine.

32. *See, e.g.*, Florida v. Jardines, 569 U.S. 1 (2013) (sniff by a narcotics dog within residential curtilage); United States v. Jones, 565 U.S. 400 (2012) (location-tracking device attached to a vehicle); United States v. Karo, 468 U.S. 705 (1984) (location-tracking device in a home).

33. *See, e.g.*, Florida v. Riley, 488 U.S. 445 (1989) (aerial surveillance of a greenhouse); United States v. Knotts, 460 U.S. 276 (1983) (location-tracking device on public roads); Smith v. Maryland, 442 U.S. 735 (1979) (numbers dialed on a telephone). While beyond the scope of this Article, it bears mentioning that the Fourth Amendment provides a limited privacy safeguard for otherwise unprotected electronic information that is held by a service provider; the service provider can assert its own constitutional privacy interest and contest the subpoena's "reasonableness." *See* Hale v. Henkel, 201 U.S. 43, 75-77 (1906) (holding that subpoenas must be reviewed for "reasonableness" under the Fourth Amendment); *In re* Horowitz, 482 F.2d 72, 75-79 (2d Cir. 1973) (reviewing constitutional limits on subpoenas); *In re* Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 130-39 (E.D. Va. 2011) (suggesting that a surveillance order served on Twitter might be reviewed for reasonableness).

34. *See infra* Appendix.

35. *See, e.g.*, United States v. Horton, 863 F.3d 1041, 1046-47 (8th Cir. 2017) (providing just one paragraph of analysis and claiming, erroneously, that the government malware retrieved the contents of the suspect's computer in sending back an IP address).

the steps involved in law enforcement hacking – each of which could trigger protections under the Fourth Amendment and the Federal Rules of Criminal Procedure.

Section B examines two Fourth Amendment perspectives on electronic evidence, corresponding to the two ways in which law enforcement agencies have conventionally obtained electronic evidence. Courts analogize a physical interaction with a device to cracking open a closed container, triggering constitutional privacy protections grounded in physical trespass and zones of privacy. By contrast, courts analyze data that are compelled from a third-party service provider – without any physical access – on a category-by-category basis, grounded in amorphous privacy expectations.

Government malware lands in a twilight zone between these two constitutional perspectives and the corresponding law enforcement techniques. Malware obtains data directly from a suspect's device – but it usually lacks any physical contact with the device. Section C tackles this doctrinal ambiguity and posits that the substantially better application of Fourth Amendment principles is that hacking is always a search.

A. The Technical Architecture of Government Malware

At a high level of generality, law enforcement hacking occurs in four distinct technical steps: delivery, exploitation, execution, and reporting.[36] This Section explains each of the steps, drawing on unsealed surveillance applications from federal investigations.

1. Delivery

The government must first deliver its malware to the target, often in a message sent to the suspect's account.[37] The communication includes a description

36. These four steps are borrowed from an influential Lockheed Martin paper on cybersecurity, which provides a valuable taxonomy of steps in the "intrusion kill chain." *See* Eric M. Hutchins et al., *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, LOCKHEED MARTIN CORP. (2011), http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf [http://perma.cc/MB7A-XUVB].

37. *See, e.g.*, Criminal Complaint at 29-33, United States v. Hernandez, No. 1:17-mj-00661 (S.D. Ind. Aug. 1, 2017) (describing malware delivery by inducing the suspect to open a video shared on Dropbox); Amended Application for a Search Warrant at 26-28, *In re* Use of a Network Investigative Technique for a Comput. Accessing Email Accounts: weknow@hotdak.net, iama.skank@yandex.com, weknow@mail2actor.com, and skankcatcher@mail2actor.com, No. 6:17-mj-00519-JWF (W.D.N.Y. Feb. 13, 2017) (describing malware delivery by causing

intended to lure the suspect into clicking a link, which directs the suspect's web browser to a website or content controlled by law enforcement. This type of malware delivery, dubbed "phishing" in the computer security field, is targeted at *specific individuals*.

A more recent law enforcement tactic involves "hidden services" that facilitate illicit activity and are only accessible to users of the Tor anonymization software.[38] In these cases, the government identifies the hidden service operator and seizes the infrastructure, but it continues to operate the service with the addition of malware.[39] When criminals interact with the website under certain triggering conditions – for example, by visiting, logging in, or going to specific webpages – the malware gets delivered. Thus, unlike a phishing attack, this type of "watering hole" attack is targeted at *any* individuals who engage in *specific behaviors*.[40]

Federal investigators have deployed a watering hole strategy in at least three investigations: Operation Torpedo in the District of Nebraska (2012),[41] an investigation of the Freedom Hosting platform in the District of Maryland

---

the suspect to execute a Microsoft Word macro); Application for a Search Warrant at 9, *In re* Network Investigative Technique (NIT) for E-mail Address 512SocialMedia@gmail.com, No. A-12-M-748 (W.D. Tex. Dec. 18, 2012) (proposing malware delivery via an email); Third Amended Application for a Search Warrant at 20, *In re* Network Investigative Technique ("NIT") for Email Address texan.slayer@yahoo.com, No. 12-sw-05685-KMT (D. Colo. Dec. 11, 2012) (same); Application and Affidavit for Search Warrant at 13-14, *In re* Search of Any Comput. Accessing Elec. Message(s) Directed to Adm'r(s) of MySpace Account "Timberlinebombinfo" and Opening Message(s) Delivered to that Account by the Gov't, No. MJ07-5114 (W.D. Wash. June 12, 2007) (proposing malware delivery via a social network message).

38. *See Tor: Hidden Service Protocol*, TOR, http://www.torproject.org/docs/hidden-services.html [http://perma.cc/9NEE-UL6E]. These services are often referred to as the "dark web."

39. The government's continued operation of criminal websites – especially child-pornography forums – has been a source of substantial controversy. *See, e.g.*, Mike Carter, *FBI's Massive Porn Sting Puts Internet Privacy in Crossfire*, SEATTLE TIMES (Aug. 27, 2016), http://www.seattletimes.com/seattle-news/crime/fbis-massive-porn-sting-puts-internet-privacy-in-crossfire [http://perma.cc/73L4-8E3Z].

40. *See* Lerner, *supra* note 28, at 40-42 (describing the phishing and watering hole strategies for government malware delivery).

41. *See* Application for a Search Warrant, *In re* Search of Computs. that Access the Website "Hidden Service A" Which Is Located at oqm66m6lyt6vxk7k.onion, No. 8:12MJ360 (D. Neb. Nov. 19, 2012) (malware delivery to visitors of the seized "Hidden Service A" service); Application for a Search Warrant, *In re* Search of Computs. that Access the Website "Hidden Service B" Which Is Located at s7cgvirt5wvojli5.onion, No. 8:12MJ359 (D. Neb. Nov. 19, 2012) (malware delivery to visitors of the seized "TB3" service); Application for a Search Warrant, *In re* Search of Computs. that Access the Website "Bulletin Board A" Located at http://jkpos24pl2r3urlw.onion, No. 8:12MJ356 (D. Neb. Nov. 16, 2012) [hereinafter *Application for "Bulletin Board A" Search Warrant*] (malware delivery to visitors of the seized "PedoBoard" service). *See generally* Kevin Poulsen, *Visit the Wrong Website and the FBI Could End Up in Your Computer*, WIRED (Aug. 5, 2014, 6:30 AM) http://www.wired.com/2014/08

(2013),[42] and Operation Pacifier (also known as the Playpen Case) in the Eastern District of Virginia (2015).[43] In the course of these investigations, the government hacked thousands of computers.[44]

These are not, to be sure, the only strategies for malware delivery. In at least one investigation, agents appear to have broken into a criminal's office and surreptitiously installed malware.[45] In a number of other cases, officers have seized a criminal's device to conduct a hack, including the high-profile conflict between Apple and the FBI about decrypting a terrorist's encrypted iPhone.[46] In conjunction with the Freedom Hosting investigation, the FBI assumed operation of an

---

/operation_torpedo [http://perma.cc/ZTG3-JZDM] (describing FBI techniques in "Operation Torpedo"). The government additionally sought and received at least one wiretap order authorizing interception of private user communications on a seized service. *See* United States v. Laurita, No. 8:13CR107, 2016 WL 4179365, at *3 (D. Neb. Aug. 5, 2016) (describing a wiretap order for private messages); United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263, at *1 (W.D. Wash. Jan. 28, 2016) (describing a wiretap order for a message board).

42. *See* Affidavit in Support of Application for a Search Warrant at 13-14, *In re* Search of Computs. that Access "Websites 1-23", No. 8:13-mj-01744-WGC (D. Md. July 22, 2013) (malware delivery to visitors of twenty-three websites related to child pornography hosted on the seized Freedom Hosting platform); *see also* Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, WIRED (Sept. 13, 2013, 4:17 PM), http://www.wired.com/2013/09/freedom-hosting-fbi [http://perma.cc/9LRE-JPH3] (describing the FBI's investigative technique).

43. *See* Affidavit in Support of Application for Search Warrant at 23-27, *In re* Search of Computs. that Access upf45jv3bziuctml.onion, No. 1:15-SW-89 (E.D. Va. Feb. 20, 2015) (proposing malware delivery to visitors of the seized "Playpen" service). Like in the Operation Torpedo investigation, the government obtained a wiretap order to intercept private messages and chats between users. Application for an Order Authorizing Interception of Electronic Communications at 4-5, No. 1:15-ES-4 (E.D. Va. Feb. 20, 2015).

44. *See Michaud*, 2016 WL 337263, at *1, *5 (noting that "the FBI may have anticipated tens of thousands of potential suspects" in the Operation Pacifier investigation, because the Playpen website had over 200,000 registered users and 1,500 daily visitors); Transcript of Oral Argument at 18, 39, United States v. Tippens, No. CR16-5110RJB (W.D. Wash. Nov. 1, 2016) (noting that the investigation involved compromising 1,432 devices inside the United States and 7,281 devices in 120 other countries and territories).

45. *See* Order at 3-6, *In re* Application of the U.S. for an Order Authorizing the Surreptitious Entry into the Premises of Merchant Servs., No. 99-4061 (D.N.J. June 9, 1999) (search warrant in *United States v. Scarfo*, 180 F. Supp. 2d 572 (D.N.J. 2001), allowing law enforcement entry to install malware on a suspect's computer).

46. *See* Ellen Nakashima, *FBI Paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone*, WASH. POST (Apr. 12, 2016), http://www.washingtonpost.com/world/nationalsecurity/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html [http://perma.cc/G6VJ-ACFU] (describing the Apple-FBI dispute); *see also In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341, 375-

email service and delivered malware to specific users.[47] In future investigations, agents might seek to gain remote access to a criminal's device by sending commands from a central management server, similar to how the FBI recently disabled criminal malware in a "botnet" consisting of compromised computers.[48] Officers could alternatively persuade a software vendor to bundle malware into an update. The differences in these delivery mechanisms can be subtle and, as discussed below, can have constitutional implications. But whatever the specifics, the critical first step will always be landing the malware on the criminal's device.

2. *Exploitation*

The second step in law enforcement hacking is exploitation. Modern technology design recognizes that software arrives from a range of sources and that not all developers are trustworthy. As a consequence, software generally executes with limited permissions: it can only access specific data and functionality on a device. Web browsers and mobile devices impose especially strict security "sandboxes," requiring that software be written in specific languages and granting access only to specific capabilities. Web browsers, for example, will usually only execute software that is written in the JavaScript language and will provide that software with access to only the stored data that are associated with the software's origin. Some sensitive capabilities, such as enabling the device's webcam and GPS, are only available with a user's affirmative consent. Other device capabilities, such as reading data from unrelated applications, are disallowed altogether. By imposing these restrictions, sandboxes both conform to and inform a user's expectations about security and privacy.

Law enforcement hacking necessarily subverts the security barriers associated with sandboxing in order to give investigators access to the data and features that they need. Developers of investigative tools identify or purchase security

76 (E.D.N.Y. 2016) (holding that the FBI could not compel Apple to assist with bypassing the lock screen on a suspect's iPhone).

47. *See* Affidavit in Support of Application for Search Warrant, *In re* Search of Computs. that Access Target E-Mail Accounts, No. 8:13-mj-01745-WGC (D. Md. Oct. 31, 2016) (targeting malware at users who access specific Tor Mail accounts); Affidavit in Support of Application for Search Warrant, *In re* Search of Computs. that Access the E-Mail Accounts Described in Attachment A, No. 8:13-mj-01746-WGC (D. Md. Oct. 31, 2016) (similar).

48. *See* Application and Affidavit in Support of an Application Under Rule 41 for a Search Warrant, *In re* Application for a Warrant Under Rule 41 of the Fed. Rules of Criminal Procedure To Disrupt the Kelihos Botnet, No. 3:17-mj-00135-DMS (D. Alaska Apr. 5, 2017).

vulnerabilities in applications that allow them to circumvent sandboxing protections. The specific security vulnerability that the government exploits and how it exploits that vulnerability depend on myriad factors, including the information that investigators seek and the software configuration used by the suspects.

In Operation Torpedo, for example, the FBI seized three illicit Tor hidden services.[49] The FBI then sought to identify Tor users who visited those websites. It did so by exploiting a vulnerability in the Adobe Flash plugin, which – at the time – many Tor users had enabled in their browser so that they could play videos embedded on webpages. By design, the Flash plugin allowed those embedded videos to initiate network communications – even if the user never saw or clicked anything in their web browser. As a security and privacy precaution, though, Flash network requests were supposed to use the exact same network settings as the operating system or web browser. In the case of a Tor user, those network settings would mean sending traffic through Tor. Because of a bug by Adobe, the protection was incomplete: certain types of network requests bypassed the network settings, circumventing Tor.[50] An FBI contractor wrote a small and invisible Adobe Flash video that did just that, and the FBI launched a watering hole attack by embedding the video on the illicit websites.[51]

A 2013 investigation by the FBI relied on a much more sophisticated exploit.[52] Working with Irish authorities, the FBI seized Freedom Hosting, a platform for illicit Tor hidden services.[53] The FBI again conducted a watering hole

49. Poulsen, *supra* note 41.

50. *See Flash Ignores FF Proxy Settings*, MOZILLA (Apr. 30, 2010), http://bugzilla.mozilla.org/show_bug.cgi?id=562880 [http://perma.cc/J93J-HQ3H].

51. *See* NIT Forensic and Reverse Engineering Report at 3, United States v. Cottom, No. 8:13-cr-00108-JFB-TDT (D. Neb. June 29, 2015) (providing a copy of the FBI software and explaining its functionality).

52. *See* Ken Buckler, *Caffsec-malware-analysis*, GOOGLE CODE (Mar. 19, 2016), http://code.google.com/p/caffsec-malware-analysis/source/default/source [http://perma.cc/6X7P-6WFN] (providing the source code and a forensic analysis of the FBI software); Vlad Tsyrklevich, *Annotation and Analysis of the Tor Browser Bundle Exploit* (Apr. 6, 2014), https://tsyrklevich.net/tbb_payload.txt [http://perma.cc/8WBX-7TB6] (providing additional forensic analysis of the FBI software); *see also Crash with Onreadystatechange and Reload*, MOZILLA (Apr. 3, 2013), https://bugzilla.mozilla.org/show_bug.cgi?id=857883 [http://perma.cc/NMD5-8MW3] (explaining the Firefox vulnerability).

53. *See* Kevin Poulsen, *Feds Are Suspects in New Malware That Attacks Tor Anonymity*, WIRED (Aug. 5, 2013), http://www.wired.com/2013/08/freedom-hosting [http://perma.cc/AAQ2-6J54].

attack by injecting malware into hidden services that resided on the seized Freedom Hosting infrastructure.[54] The specific mechanism for the FBI's hacking differed, though. The FBI (or, more likely, a contractor) discovered that the Mozilla Firefox web browser included a serious memory management vulnerability. A clever website could load an unsandboxed application into Firefox's memory, then trick Firefox into executing the application. The result was that a website could take over Firefox, gaining near-total control over the computer. Whenever a user visited one of the Freedom Hosting websites with a vulnerable version of Firefox, the FBI's software would take over.[55]

3. *Execution*

Once law enforcement has circumvented security protections, its software executes. A simple instance of malware, like in Operation Torpedo, might merely note the time that the software executed, collect information about the operating system and processor, and then send a network request that includes the device's IP address.[56]

More sophisticated malware can retrieve additional identifying information via a device's operating system. For example, the FBI's Freedom Hosting malware collected a computer's name and the unique identifier that the computer's manufacturer assigned to its network card.[57]

Malware that the FBI deployed in 2015 as part of Operation Pacifier went slightly further. According to an unsealed surveillance application, the software stored information about whether the malware had previously executed and retrieved the name of the user currently logged into the computer.[58]

---

54. *See* Poulsen, *supra* note 42.

55. The precise triggering conditions for this malware deployment remain ambiguous. See *infra* notes 200 and 256 and accompanying text.

56. *See* NIT Forensic and Reverse Engineering Report, *supra* note 51, at 3 (calling the Adobe Flash interfaces Capabilities.os to determine the operating system, Capabilities.cpuArchitecture to determine the processor architecture, and Lib.current.loaderInfo.parameters.id to retrieve a unique session identifier).

57. *See Analysis of the Tor Browser Bundle Exploit Payload*, VLAD TSYRKLEVICH (Apr. 6, 2014), http://tsyrklevich.net/tbb_payload.txt [http://perma.cc/VV8L-DJL7] (calling the Windows Sockets interface gethostname() to determine the computer's configured name and the interface gethostbyname() to determine the computer's local IP address, then calling the IP Helper interface SendARP to determine the computer's MAC address).

58. Attachment B to Application for a Search Warrant, *In re* Search of Computs. that Access upf45jv3bziuctml.onion, No. 1:15-SW-89 (E.D. Va. Feb. 20, 2015).

Some FBI malware goes much further yet. According to two recent district court opinions, certain configurations of FBI software can remain resident and operational on a suspect's computer for extended periods and can access files, log keystrokes, intercept communications, track location, and even enable the computer's camera.[59]

4. *Reporting*

Finally, as the law enforcement software executes on a suspect's device, it phones home to report investigative information. Any government-controlled server will work. In the Operation Torpedo investigation, for instance, an FBI server received malware reports using proprietary webserver software.[60] In most cases, an inexpensive server running free software would be more than adequate.

* * *

These four steps – delivery, exploitation, execution, and reporting – are fundamental to the operation of government malware. And each step could potentially trigger Fourth Amendment protections. Part II will return to the delivery and execution steps in evaluating when law enforcement hacking becomes a Fourth Amendment search and how long the search lasts.

The remainder of this Part focuses on the exploitation and reporting steps, for two reasons. First, the most common form of government malware – used to identify Tor users – does not trigger the Fourth Amendment at delivery, and it executes nearly instantaneously.[61] If there is any constitutional privacy protection associated with this form of malware, it must reside in the exploitation and reporting steps. Second, for this type of law enforcement hacking, the exploitation and reporting steps implicate two distinct perspectives on Fourth Amendment privacy; exploitation involves intruding into a suspect's electronic device (without physical access), while reporting involves extracting discrete categories of information. The courts are deeply divided about how to reconcile the positive law, and about half of them are getting it wrong.[62]

---

59. *See* United States v. Laurita, No. 8:13CR107, 2016 WL 4179365, at *3 (D. Neb. Aug. 5, 2016); *In re* Warrant To Search a Target Comput. at Premises Unknown, 958 F. Supp. 2d 753, 755-56 (S.D. Tex. 2013).

60. *See* NIT Forensic and Reverse Engineering Report, *supra* note 51, at 4-8 (describing and analyzing the FBI's backend server code, dubbed Cornhusker).

61. *See infra* Sections II.A, II.D.

62. *See infra* Appendix (collecting and comparing cases).

B. *Conventional Methods for Obtaining Electronic Evidence and Corresponding Perspectives on Fourth Amendment Privacy*

Law enforcement agencies have traditionally relied on two methods for obtaining electronic evidence, both of which long predate government hacking. Meanwhile, Fourth Amendment doctrine has developed to reflect two corresponding conceptions of information privacy.

First, investigators might physically seize a device and extract data stored in the device's memory. They might conduct a forensic examination of a desktop computer's hard disk, for example, or scroll through the photos on a suspect's smartphone. Courts have traditionally analyzed these investigative techniques from a *device-centric* perspective and applied a line of cases – rooted in English common law – that safeguards the integrity of personal *spaces*.

Second, investigators might obtain electronic evidence from third-party service providers. They might operate a wiretap on a telephone line, for instance, or compel an email service to disclose stored messages. Courts analyze these investigative techniques from a *data-centric* perspective, tracing to the seminal 1967 opinion in *Katz v. United States*,[63] and emphasize the *information* that the government obtains.

1. *Physical Access to an Electronic Device and the Device-Centric Perspective*

Since the nineteenth century, the Fourth Amendment's procedural safeguards have unambiguously applied to closed containers.[64] Most modern opinions frame this protection in the familiar language of *Katz*: a person has a reasonable expectation of privacy in the contents of a sealed package, such that a government intrusion constitutes a Fourth Amendment search.[65] Courts are especially protective of the home, which has long been at the core of Fourth Amendment privacy protection.[66]

---

63. 389 U.S. 347 (1967).

64. *See Ex parte* Jackson, 96 U.S. 727, 735 (1877) ("[R]egulations . . . cannot be enforced in a way which would require or permit an examination into . . . sealed packages . . . without warrant, issued upon oath or affirmation, in the search for prohibited matter . . . .").

65. *E.g.*, United States v. Chadwick, 433 U.S. 1, 11 (1977) ("By placing personal effects inside a double-locked footlocker, respondents manifested an expectation that the contents would remain free from public examination.").

66. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001) ("[I]n the case of the search of the interior of homes – the prototypical and hence most commonly litigated area of protected privacy – there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*."); United States v. U.S.

Some opinions on closed containers have also emphasized property rights, especially following the Supreme Court's recent reinvigoration of trespass as a Fourth Amendment trigger in *United States v. Jones* and *Florida v. Jardines*.[67] Merely touching a closed container for the purpose of obtaining information may be sufficient to trigger Fourth Amendment search protections.[68]

Reasoning by analogy, courts have extended these closed-container protections to physical searches of electronic devices. A computer, the thinking goes, is an electronic (and exceptionally capacious) filing cabinet.[69] The analogy has its shortcomings, to be sure. Because of the extraordinary volume and sensitivity of personal data stored on electronic devices, courts have exempted devices from conventional limits on closed-container privacy protections. For example, courts have declined to eliminate privacy protections when a device is searched incident to arrest,[70] when a device is left in an automobile,[71] or when incriminating data

---

Dist. Court (*Keith*), 407 U.S. 297, 313 (1972) ("[P]hysical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed . . . .").

67. *See* Florida v. Jardines, 569 U.S. 1, 5-12 (2013) (following *Jones* and applying it to a drug-sniffing dog on residential curtilage); United States v. Jones, 565 U.S. 400, 404-11 (2012) (noting a property-based conception of the Fourth Amendment, and applying it to the attachment of a GPS-tracking device); *see also* Entick v. Carrington, 19 Howell's St Trials 1029 (CP 1765) (establishing government liability for trespasses to real and personal property). Whether this trespass test applies to purely electronic searches remains ambiguous. *Jones*, 565 U.S. at 426 (Alito, J., concurring) ("[T]he Court's reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact . . . .").

68. *See, e.g.*, United States v. Thomas, 726 F.3d 1086, 1092-93 (9th Cir. 2013) (suggesting that police dog contact with the outside of a toolbox, combined with a sniff test for the presence of drugs, could constitute a Fourth Amendment search). Similarly, manipulating or retaining a container could constitute sufficient interference with possessory interests to trigger Fourth Amendment seizure protections. *E.g.*, State v. Kelly, 708 P.2d 820, 823-24 (Haw. 1985).

69. *See, e.g.*, United States v. Andrus, 483 F.3d 711, 718-19 (10th Cir. 2007) (assessing appropriate Fourth Amendment analogies for computer systems, and concluding that "it seems natural that computers should fall into the same category as suitcases, footlockers, or other personal items that command[] a high degree of privacy" (alteration in original) (citation omitted)); *see also* United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers."); Trulock v. Freeh, 275 F.3d 391, 402-04 (4th Cir. 2001) (analogizing password-protected files on a shared computer to a locked footlocker); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) ("Home owners would of course have a reasonable expectation of privacy in their homes and in their belongings—including computers—inside the home.").

70. *See* Riley v. California, 134 S. Ct. 2473, 2488-95 (2014) (holding that the search incident to arrest doctrine does not apply to data stored on mobile phones).

71. *See* United States v. Burgess, 576 F.3d 1078, 1087-90 (10th Cir. 2009) (suggesting that the automobile search exception to the warrant requirement may not apply to computers); Wertz

are in plain view.[72] But in the first instance, when determining whether a search has taken place, the closed-container analogy has continuing value and vitality.

2. *Remote Access to Information via a Third Party and the Data-Centric Perspective*

In *Katz v. United States* the Supreme Court held, for the first time, that the scope of the Fourth Amendment is not solely delineated by physical barriers. Instead, the Court articulated a new conception of Fourth Amendment information privacy that emphasizes the data that the government obtains, rather than the spaces that the government invades. "[T]he Fourth Amendment protects people, not places," the Court memorably explained.[73] *Katz* itself dealt with a positive expansion of constitutional privacy protection, holding that a telephone wiretap constitutes a search even without a physical trespass to install the wiretap. Congress and the courts have uniformly interpreted *Katz* to cover all real-time interceptions of communications content, and recent lower court opinions have similarly recognized Fourth Amendment protection when the government accesses stored communications content from a service provider.[74]

---

v. State, 41 N.E.3d 276, 280-82 (Ind. Ct. App. 2015) (holding that the automobile search exception does not apply to electronic devices).

72. *See* United States v. Carey, 172 F.3d 1268, 1272-74 (10th Cir. 1999) (declining to apply the plain view doctrine to computer searches in which investigators opened files not covered by a warrant).

73. Katz v. United States, 389 U.S. 347, 351 (1967).

74. *See* United States v. Warshak, 631 F.3d 266, 283-88 (6th Cir. 2010) (holding that government access to stored email content is a Fourth Amendment search because, among other reasons, any other rule would be inconsistent with Fourth Amendment protection for real-time interception of email content). Although *Warshak* is only binding within the Sixth Circuit, a number of courts have cited the opinion with approval. *See, e.g.*, United States v. Ackerman, 831 F.3d 1292, 1306 (10th Cir. 2016); United States v. Graham, 824 F.3d 421, 433 (4th Cir. 2016); United States v. Carpenter, 819 F.3d 880, 887 (6th Cir. 2016); Vista Marketing, LLC v. Burkett, 812 F.3d 954, 969 (11th Cir. 2016). No court has rejected the holding.

In the years following *Warshak*, the executive branch adopted the position that warrant protections are appropriate for stored content. *See ECPA (Part 1): Lawful Access to Stored Content: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec., and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 20 (2013) (statement of Elana Tyrangiel, Acting Assistant Att'y Gen. of the United States); *A Response to Your Petition on ECPA*, WHITE HOUSE, http://petitions.obamawhitehouse.gov/petition/reform-ecpa-tell-government-get-warrant [http://perma.cc/X322-NF6R]. In 2013, the Department of Justice established a formal policy of obtaining a search warrant before accessing stored communications in criminal investigations. H.R. REP. NO. 114-528, at 9 (2016). At present, nearly every major online service requires a search warrant before disclosing customer content to a law enforcement agency. Nate Cardozo et al., *Who Has Your Back? Protecting Your Data from Government Requests*, ELEC.

Many information privacy opinions have, however, invoked the *Katz* test in a negative manner. Where a piece of information has not been kept *entirely* secret from third-party businesses or public vantage points, courts have generally declined to recognize constitutional privacy interests.[75] Courts have held that there is categorically no reasonable expectation of privacy—and therefore no Fourth Amendment protection—in subscriber information,[76] communications metadata,[77] and geolocation records.[78] Congress has acted in accord with these views, developing a (notoriously complex) regulatory scheme within the Electronic Communications Privacy Act that generally allows for warrantless law enforcement access to these types of data.[79]

FRONTIER FOUND. 8 (2015), http://www.eff.org/files/2015/06/18/who_has_your_back_2015_protecting_your_data_from_government_requests_20150618.pdf [http://perma.cc/M6GS-6ERL].

75. *See, e.g.*, Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1086-87 ("The Court's current conception of privacy is as a form of total secrecy . . . . Since information maintained by third parties is exposed to others, it is not private, and therefore not protected by the Fourth Amendment."). Courts and commentators have developed a range of terms for describing these doctrines, including the "third-party doctrine," "metadata doctrine," and "public movements doctrine." Whatever the terminology, the underlying rationales are essentially shared.

76. *See, e.g.*, United States v. Perrine, 518 F.3d 1196, 1204-05 (10th Cir. 2008) (holding that communications subscriber information is not protected by the Fourth Amendment and collecting similar cases).

77. *See, e.g.*, United States v. Forrester, 512 F.3d 500, 509-11 (9th Cir. 2008) (concluding that surveillance of non-content aspects of communications—i.e., metadata—does not implicate the Fourth Amendment).

78. *See, e.g.*, United States v. Thompson, No. 15-3313, 2017 WL 3389368, at *4-9 (10th Cir. Aug. 8, 2017) (holding that the third-party doctrine precludes Fourth Amendment protection for retrospective cell-site location information); *Graham*, 824 F.3d at 424-38 (4th Cir. 2016) (same); *Carpenter*, 819 F.3d at 886-90 (6th Cir. 2016) (same); United States v. Davis, 785 F.3d 498, 505-18 (11th Cir. 2015) (same); *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 608-15 (5th Cir. 2013) (same); *see also* United States v. Wallace, 857 F.3d 685 (5th Cir.) (reaching the same conclusion for prospective cell-site location information, though the opinion was withdrawn and replaced because the case actually involved GPS information), *withdrawn*, 866 F.3d 605 (5th Cir. 2017). *But see, e.g.*, Tracey v. State, 152 So. 3d 504, 511-26 (Fla. 2014) (reaching the opposite conclusion for prospective cell-site location information and reserving judgment on retrospective information). The Supreme Court is reviewing *Carpenter* in the current term, and, as discussed *infra* note 122 and accompanying text, is widely expected to find at least some measure of Fourth Amendment protection for geolocation records.

79. *See* 18 U.S.C. § 2703(c)(2) (2012) (authorizing law enforcement access to subscriber records and telephone metadata with a grand jury or administrative subpoena); *id.* § 2703(d) (establishing an intermediate court order for non-content records, including internet communica-

C. *Obtaining Electronic Evidence by Hacking*

Law enforcement hacking thus poses a Fourth Amendment conundrum. It shares a key feature of physical device searches: the government obtains data directly from the suspect's device. But it also shares key features of compelling data from a service provider: there is no physical contact with the suspect's property, and the data that the government obtains can be conceptually divided into content and metadata categories. The following subsections analyze the Fourth Amendment issues associated with law enforcement hacking, beginning with easy fact patterns and then turning to challenging scenarios.

1. *The Easy Scenarios: Physical Access or Content*

Before turning to the difficult fact patterns, it is important to briefly explain what is not in dispute. When the delivery phase of malware involves law enforcement officers *physically* interacting with a suspect's device, they unambiguously engage in a Fourth Amendment search. As explained above, courts have consistently drawn an analogy between physically interacting with an electronic device and opening a closed container, grounding their analysis in *Katz* (and more recently *Jones*). Physical installation of malware equates to cracking open a closed container, rendering it a Fourth Amendment search.

Even without the closed-container analogy, these fact patterns are easy to resolve under a straightforward application of *Jones*. In three recent opinions, the Supreme Court has grappled with a physical trespass to obtain data that are otherwise constitutionally unprotected. And, in all three cases, the Court has treated law enforcement's trespassory conduct as sufficient to implicate the Fourth Amendment.

United States v. Jones evaluated the constitutional protections associated with a GPS tracking device attached to a suspect's car.[80] A majority of the Court held that, regardless of whether there is a cognizable Fourth Amendment interest in a person's location, physically trespassing against a car constitutes a search.[81]

In *Florida v. Jardines*, the Court assessed police use of drug-sniffing dogs on real property.[82] The majority extended *Jones*, reasoning that stepping onto a

tions metadata and device geolocation); *id.* § 2709 (2012) (granting limited authority for administrative subpoenas, commonly referred to as national security letters, for subscriber records and telephone metadata).

80. 565 U.S. 400, 402 (2012).

81. *Id.* at 406-11.

82. 569 U.S. 1, 3 (2013).

porch to conduct a dog sniff is sufficient trespass to become a search, even if there is no Fourth Amendment protection against a dog sniff alone (because it solely reveals illegal activity).[83]

Most recently, *Riley v. California* considered police searches of mobile phones incident to the arrest of two suspects.[84] As a fallback argument in the case, the United States argued that a suspect has a diminished privacy interest in the call log stored on his phone because it solely consists of metadata.[85] Both the majority and the concurrence rejected that position, implicitly holding that when police officers tap away at a suspect's phone they always conduct a search – regardless of the specific information that they obtain.[86] *Jones*, *Jardines*, and *Riley* unambiguously establish that a physical trespass to obtain information is a search, even when the information is otherwise constitutionally unprotected.

Analyzing the Fourth Amendment implications of malware is also easy when the reporting step transmits the content of a communication or a file. Since the seminal 2010 opinion in *United States v. Warshak*, courts have consistently held that the Fourth Amendment protects content held by third-party service providers.[87] It would be an absurd result if lesser privacy protections applied when law enforcement officers obtain the same information through a more intrusive mechanism (hacking). The government does not appear to have advanced this position in any case, and, as discussed further below, it has consistently (albeit implicitly) conceded that hacking to obtain content is a Fourth Amendment search.

---

83. *Id.* at 5-12.

84. 134 S. Ct. 2473, 2480 (2014).

85. *Id.* at 2492-93.

86. *Id.*

87. *In re* Search of Premises Known As: Three Hotmail Email Accounts, No. 16-MJ-8036-DJW, 2016 WL 1239916, at *8 (D. Kan. Mar. 28, 2016) ("[E]very court . . . that has participated in this discussion [of Fourth Amendment protections for electronically stored content] agrees . . . individuals have a right to privacy with respect to email . . . ."); *see, e.g.*, Quon v. Arch Wireless Operating Co., 529 F.3d 892, 906-08 (9th Cir. 2008) (concluding that the Fourth Amendment protects archived text messages); *In re* Search of Info. Associated with the Facebook Account Identified by the Username Aaron.Alexis that Is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1, 6 (D.D.C. 2013) (assuming that the Fourth Amendment protects private content on a social network).

2. *The Hard Scenario: Remote Access to Metadata*

So much for the easy cases. Malware is much more difficult to evaluate under the Fourth Amendment when the delivery phase does not involve physical contact with the suspect's device and the reporting phase does not include any content information.

This category includes the most common type of law enforcement hacking: the FBI's identification of Tor users. The key data that the malware reports is a suspect's IP address.[88] Law enforcement officers can then use the IP address to learn the suspect's identity and physical address.[89] Courts have consistently held that an IP address is constitutionally unprotected metadata, much like a telephone number.[90] Thus, the typical deployment of government malware is also the most constitutionally challenging.

The following subsections attempt to provide the best possible articulation of two positions on how the Fourth Amendment maps onto this scenario. The first viewpoint, advanced by the United States in a number of district court filings, is that the Fourth Amendment does not apply because it does not regulate de minimis or electronic intrusions to obtain metadata.

The opposing perspective, advanced by numerous criminal defendants, is that the Fourth Amendment does apply in this scenario and protects the electronic equivalent of a device's physical integrity. I locate much stronger support for this "logical integrity" principle in both positive law and policy considerations.

a. *A Plausible Position: No Fourth Amendment Protection*

The usual position of the United States government has been that Fourth Amendment protections associated with government malware are determined

88. The government's Tor identification malware collects additional information that could trigger constitutional scrutiny, but that information is not typically used in prosecution.

89. They do so by issuing a reverse Domain Name System query (which is free) to find the corresponding ISP and then subpoenaing the ISP. *See, e.g.*, United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *3 (C.D. Cal. Aug. 8, 2016) (denying defendant's motion to suppress evidence in a case where defendant's name and address were discovered via a subpoena to Time Warner Cable); United States v. Darby, 190 F. Supp. 3d 520, 529 (E.D. Va. 2016) (subpoena to Verizon).

90. *See, e.g.*, United States v. Ulbricht, 858 F.3d 71, 94-98 (2d Cir. 2017); United States v. Suing, 712 F.3d 1209, 1213 (8th Cir. 2013); United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008); United States v. Forrester, 512 F.3d 500, 509-10 (9th Cir. 2008).

exclusively by the data that the malware reports.[91] If the malware only sends back metadata, it is not a Fourth Amendment search, and it is not constitutionally regulated. If the malware transmits real-time audio, video, or electronic communications, then heightened Fourth Amendment protections (sometimes dubbed "super-warrant" protections) will apply.[92]

According to documents released under the Freedom of Information Act, the government's current position dates to the mid-2000s, when FBI agents and

---

91. *E.g.*, United States' Response in Opposition to Defendant's Motion To Suppress Evidence at 10-13, United States v. Schuster, No. 1:16-CR-051, 2017 WL 1154088 (S.D. Ohio Sept. 1, 2016) (arguing that there is no Fourth Amendment protection for government malware that reports an IP address); Government's Opposition to Defendant's Motion To Suppress Evidence at 8-12, United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436 (C.D. Cal. July 11, 2016) (similar); *see also* United States v. Laurita, No. 8:13CR107, 2016 WL 4179365, at *6 (D. Neb. Aug. 5, 2016) (explaining the government's withdrawal of a stipulation that using malware to obtain an IP address constitutes a Fourth Amendment search). The United States also adopted this position in an Eighth Circuit challenge to evidence arising from the Operation Torpedo investigation. Brief of Appellee at 27-28, United States v. Welch, No. 15-1993 (8th Cir. Aug. 12, 2015). The government's invocation of this argument has not, however, been uniform. *See, e.g.*, Government's Reply Brief at 22 n.12, United States v. Horton, No. 16-3976, 2017 U.S. Dist. LEXIS 44757 (8th Cir. Jan. 9, 2017) ("[Defendant] argues . . . that he had a reasonable expectation of privacy in his IP address and the information stored on his computer, but we have not suggested otherwise."); United States' Response in Opposition to Defendant's Supplemental Motion To Suppress at 3 n.2, United States v. Gaver, No. 3:16-CR-88 (S.D. Ohio Dec. 16, 2016) (withdrawing its earlier argument that obtaining an IP address was not a search); *see also* Orin Kerr, *What's Missing in the Government's Briefs in the Playpen Warrant Cases*, WASH. POST: VOLOKH CONSPIRACY (Feb. 20, 2017), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/02/20/whats-missing-in-the-governments-briefs-in-the-playpen-warrant-cases [http://perma.cc/W9U5-QGUN] (noting that the United States did not advance this argument in three appeals arising from the Operation Pacifier investigation). The United States also suggested – but then dropped – a similar argument before the Supreme Court in the context of searching mobile phones incident to arrest. *Compare* Brief for Petitioner at 42, Riley v. California, 134 S. Ct. 2473 (2014) (No. 13-212) (suggesting that a suspect has no reasonable expectation of privacy in his mobile phone's stored call log), *aff'g* United States v. Wurie, 728 F.3d 1 (1st Cir. 2013), *with* Reply Brief for Petitioner at 7, 15-16, *Riley*, 134 S. Ct. 2473 (No. 13-212) (clarifying that a suspect has a reasonable expectation of privacy in his mobile phone's stored call log, but that a search of the call log incident to arrest would be "reasonable").

92. *See Laurita*, 2016 WL 4179365, at *3 (describing a super-warrant application for an "Order Authorizing the Surreptitious Installation of Electronic Keyboard Keystroke and Computer Screen Capture Recording Devices To Collect Computer Keyboard Keystrokes and Computer Screen Captures . . ."); *see also* Memorandum from David Bitkower, Deputy Assistant Att'y Gen., U.S. Dep't of Justice, Criminal Div., to Judge Reena Raggi, Chair, Advisory Comm. on Criminal Rules, at 9 (Dec. 22, 2014) (on file with author) (noting that the Wiretap Act, which is the statutory implementation of *Berger v. New York*'s super-warrant doctrine, applies to government malware that intercepts electronic communications).

counsel argued for scoping Fourth Amendment protection according to the content-metadata distinction.[93] The warrant application in the 2007 Timberline High School investigation, for example, expressly declined to concede that law enforcement hacking to obtain identifying information would constitute a search and necessitate a warrant.[94]

The Department of Justice appears to have held a different opinion until recently, at least internally. Guidance from the Computer Crime and Intellectual Property Section, dating back to a 2002 memorandum, has consistently recommended a search warrant for law enforcement hacking.[95] In 1999, the DOJ led a federal interagency working group that similarly recognized that malware used

---

93. *See* Email from [Redacted] to [Redacted] Re: IPAV (May 11, 2006), *in* 3 ELEC. FRONTIER FOUND., CIPAV FOIA RELEASE 1, https://www.eff.org/files/filenode/cipav/fbi_cipav-03.pdf [http://perma.cc/9GZR-RD2G] ("I think that you most likely were told that a simple IPAV would be used initially, in which case I would agree with your initial analysis. [Redacted, apparent description of additional hacking steps to provide contrast.] This clearly requires a search and therefore a warrant and/or consent."); Email from [Redacted] to [Redacted] Re: [Redacted] (Aug. 24, 2005), *in* 14 ELEC. FRONTIER FOUND., CIPAV FOIA RELEASE 36, https://www.eff.org/files/filenode/cipav/fbi_cipav-14.pdf [http://perma.cc/7EA7-XRJM] ("I still think that use of [redacted] is consensual monitoring without need for process . . . . That said, I will try to contort my mind into a different position if you still think otherwise."); Email from [Redacted] to [Redacted] (Aug. 23, 2005), *in* 3 ELEC. FRONTIER FOUND., *supra*, at 44 (acknowledging that whether a search warrant is required "is a hotly debated issue, and as of yet there is no policy guidance issued"); Email from [Redacted] to [Redacted] Re: UCO Proposal (Dec. 8, 2004), *in* 1 ELEC. FRONTIER FOUND., CIPAV FOIA RELEASE 4, https://www.eff.org/files/filenode/cipav/fbi_cipav-01.pdf [http://perma.cc/WNX8-EKA8] ("We all know that there are IPAVs and then there are IPAVs. Of course the technique can be used in a manner that would require a court order. We need to know how/when to draw the line for obvious reasons."); *id.* at 5 ("I don't necessarily think a search warrant is needed in all [hacking] cases . . . ."); Email from [Redacted] to [Redacted] Re: UCO Proposal (Dec. 1, 2004), *in* 1 ELEC. FRONTIER FOUND., *supra*, at 9 ("[T]he safest course is to secure a warrant, though one might arguably not be required . . . ."); Email from [Redacted] to [Redacted] Re: IPAVs (Aug. 4, 2004), *in* 1 ELEC. FRONTIER FOUND., *supra*, at 41 ("There is an argument that at least the simplest IPAV is essentially akin to a [redacted] command and that under this principle may be used without a court order.").

94. Application and Affidavit for Search Warrant, *supra* note 4, at 2 n.2 ("In submitting this request, the Government respectfully does not concede that . . . a reasonable expectation of privacy is abridged by the use of this communication technique, or that the use of this technique to collect a computer's IP address, MAC address or other variables that are broadcast by the computer whenever it is connected to the Internet, constitutes a search or seizure.").

95. *See* Email from [Redacted] to [Redacted] Re: UCO Proposal (Dec. 1, 2004), *in* 1 ELEC. FRONTIER FOUND., *supra* note 93, at 9 ("According to guidance issued by DOJ CCIPS, DOJ has 'consistently advised AUSAs and agnets [sic] proposing to use IPAVs to obtain a warrant to avoid the exclusion of evidence.' This opinion is dated March 7, 2002, written by [redacted].").

to identify suspects could trigger constitutional privacy protections.[96] In the early Operation Torpedo litigation, federal prosecutors even stipulated that law enforcement hacking is necessarily a Fourth Amendment search – but they withdrew the stipulation once courts began to conclude otherwise.[97]

It is not apparent whether federal law enforcement agents have ever deployed malware without obtaining a search warrant. FBI personnel have emphasized that the agency is not bound by the DOJ's informal legal conclusions,[98] and one email hints at past instances of hacking without first obtaining a warrant.[99]

The government's inclination against recognizing Fourth Amendment protection is understandable. In the most common type of law enforcement hacking, agents could take action without the roadblocks of developing and demonstrating probable cause. There is, furthermore, a colorable case law foundation for the government's position. In several scenarios involving modern investigative techniques, courts have conducted a Fourth Amendment analysis that emphasizes the information that law enforcement obtains, rather than how it obtains it.

This Section attempts to articulate the best precedential basis for the government's preferred doctrinal result. Each line of cases plausibly supports the government's position, but even if each line of cases is good law – which is dubious – each can be readily explained by applying established Fourth Amendment principles. Therefore, while these cases are consistent with the government's doctrinal views, they ultimately lend very weak support to the government's position. The balance of this Section sketches each line of cases, then offers an alternative, principled explanation for each.

---

96. U.S. DEP'T OF JUSTICE, ONLINE INVESTIGATIONS WORKING GRP., ONLINE INVESTIGATIVE PRINCIPLES FOR FEDERAL LAW ENFORCEMENT AGENTS 20 (1999) (noting that "agents must be careful to use [identifying] information-gathering tools only as conventionally permitted and not in a manner unauthorized by the system (as by exploiting design flaws . . .)").

97. *Compare* United States v. Pierce, No. 8:13CR106, 2014 WL 5173035, at *8 (D. Neb. Oct. 14, 2014) (describing the stipulation in the Operation Torpedo cases), *with Laurita*, 2016 WL 4179365, at *6 (describing the government's withdrawal of its stipulation).

98. *See* Email from [Redacted] to [Redacted] Re: UCO Proposal (Dec. 8, 2004), *in* 1 ELEC. FRONTIER FOUND., *supra* note 93, at 4 ("[I]t is my understanding that there is a disagreement on the status of the IPAV between what FBI/OGC says and what DOJ/CCIPS [sic]. If OGC will set out a policy on this, we will be glad to rely on it.").

99. *See* Email from [Redacted] to [Redacted] Re: IPAV/CIPAV (Nov. 22, 2004), *in* 1 ELEC. FRONTIER FOUND., *supra* note 93, at 24 ("He wants all [special agents] to know that [the Office of the General Counsel] expects a [search warrant] for all IPAV/CIPAV applications (no getting around [the Operational Technology Division] by going to another Division that currently doesn't follow CCIPS guidance on this point).").

i. Mobile Phone Location Tracking

One line of relevant cases arises from mobile phone location tracking. Some courts have reasoned that, because police officers could track a suspect's public movements without triggering Fourth Amendment safeguards (i.e., by tailing), they may obtain the suspect's movements electronically without procuring a warrant.[100]

Opinions that consider government access to ordinary cell-site location information – whether retrospective or prospective – tend to minimize this reasoning. The majority view in those cases is that cell-site location information is a routine business record knowingly disclosed to a third party (i.e., the suspect's phone company), so it is exempt from Fourth Amendment protection.[101]

The public movements argument is much more prominent in cases that involve generating new location data from mobile phones by, for example, causing the creation of new cell-site location records or by activing GPS functionality that is built-in for emergency purposes.[102] The third-party disclosure argument is strained in these cases, because there is no routine and voluntary creation of a business record. Instead, the government affirmatively causes the suspect's device to generate incriminating location data.[103] Some courts considering these

---

100. *See, e.g.*, United States v. Forest, 355 F.3d 942, 951-52 (6th Cir. 2004), *vacated*, 543 U.S. 1100 (2005).

101. *See supra* note 78 (collecting cases on cell-site location information and the Fourth Amendment).

102. Courts have not been consistent in their terminology for these practices. *See, e.g.*, United States v. Skinner, 690 F.3d 772, 787 (6th Cir. 2012) (suggesting that "ping" data is cell-site location information and distinct from GPS data); United States v. Caraballo, 963 F. Supp. 2d 341, 346 (D. Vt. 2013), *aff'd*, 831 F.3d 95 (6th Cir. 2016) (using the same term to reference both cell-site location information and GPS data). Courts have also been spotty on the technical details of these practices. A panel of the Fifth Circuit, for example, recently misunderstood an instance of GPS tracking as an instance of prospective cell-site location information tracking. *See* United States v. Wallace, 857 F.3d 685 (5th Cir.) (reaching the same conclusion for prospective cell-site location information, but later withdrawing and replacing the decision because the case actually involved GPS information), *withdrawn*, 866 F.3d 605 (5th Cir. 2017).

103. The third-party doctrine rationale is even further strained when the government collects location data directly, such as with a "cell-site simulator" device (commonly called an "IMSI catcher" or "Stingray"). *See* Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183 (2014) (explaining cell-site simulator technology and surveying district court opinions). Given the relative paucity of case law on cell-site simulators – to date, not one federal appellate court has rigorously reviewed the technology – the discussion above emphasizes other mobile-phone tracking techniques. *See* United States v. Ellis, No. 13-CR-00818 PJH, 2017 WL 3641867, at *1-7 (N.D. Cal. Aug. 24, 2017) (determining that police use of a cell-site simulator is a Fourth Amendment search); United States v. Lambis, 197 F. Supp. 3d 606, 609-11, 614-16 (S.D.N.Y. 2016) (same); Jones v. United States,

investigative techniques have consequently emphasized the types of data that the government obtains.

A pair of Sixth Circuit opinions exemplify this line of argument. In a 2004 ruling, a three-judge panel concluded that government-generated mobile phone location data is "simply a proxy" for a police tail, and does not implicate the Fourth Amendment.[104] Another panel reaffirmed that holding in 2012, elaborating that "[u]sing a more efficient means of discovering [the same public location] information does not amount to a Fourth Amendment violation."[105] It bolstered its conclusion with the observation that "[l]aw enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system."[106]

A parallel argument can easily be constructed for government malware. Law enforcement hacking, the reasoning goes, is "simply a proxy" for subpoenaing unprotected network configuration information. "Using a more efficient means of discovering [the same network configuration] information does not amount to a Fourth Amendment violation." And to hold otherwise would allow criminals to "circumvent[] the justice system," rewarding them with heightened constitutional protections when they employ anonymization software.

ii. ISP Surveillance

Another line of cases involves surveilling internet usage. In order to monitor a suspect's web browsing and email metadata, investigators sometimes examine the network data flowing through the suspect's ISP. In these instances of surveillance, investigators rely on a "pen/trap" order, which involves substantially less procedural protection than a search warrant.[107] Law enforcement officers serve

168 A.3d 703, 711-13 (D.C. 2017) (same); State v. Andrews, 134 A.3d 324, 339-52 (Md. Ct. Spec. App. 2016) (same); *see also* United States v. Patrick, 842 F.3d 540, 543-44 (7th Cir. 2016) (noting a split in authority on the issue).

104. *Forest*, 355 F.3d at 951.

105. *Skinner*, 690 F.3d at 779.

106. *Id.* at 778. While I have many reservations about the *Skinner* opinion, I find this part particularly objectionable, since it has the law backward. Making a privacy-protecting choice *increases* a person's Fourth Amendment protection (i.e., his or her reasonable expectation of privacy). Electing to have a conversation indoors, for instance, results in higher privacy safeguards than holding the chat in public.

107. When seeking email metadata prospectively, law enforcement officers much more commonly serve a pen/trap order on the suspect's email service (e.g., Google) and receive a real-time feed in response. Since this form of email surveillance does not implicate competing Fourth

the order on the suspect's ISP (e.g., Comcast). They then configure a filtering device on the ISP's network, which sifts through the suspect's traffic flows, extracts web browsing and email metadata, and sends back the results.

Applying the Fourth Amendment doctrine for third-party service providers is not straightforward.[108] From an absolute perspective, the suspect's web and email metadata are categorically unprotected, so law enforcement officers may obtain it without a warrant. From a relative perspective, though, the suspect's ISP has no legitimate reason for peering into his network traffic. From the ISP's vantage point, a suspect's web and email metadata could be considered communications content, since they play no part in routing traffic.[109] Indeed, when ISPs have previously conducted "deep packet inspection" on web metadata, they have been subjected to widespread consumer privacy criticism and to attempted regulation by the Federal Communications Commission.[110]

Lower court opinions on metadata surveillance have tended to favor the absolute perspective, holding that interception of metadata via a communications carrier is exempt from Fourth Amendment protection, even if those metadata are intended for processing by another party.[111] Judicial analysis has emphasized

---

Amendment perspectives, I focus solely on ISP-based email surveillance. The ISP-based approach to email surveillance has also become less common owing to the adoption of secure email transfer and mobile devices.

108. *See* Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends* Katz, Smith, *and Electronic Surveillance Law*, 30 HARV. J.L. & TECH. 1 (2016) (describing multiple possible approaches to the content/metadata distinction); Orin Kerr, *Relative vs. Absolute Approaches to the Content/Metadata Line*, LAWFARE (Aug. 25, 2016, 4:18 PM), http://www.lawfareblog.com/relative-vs-absolute-approaches-contentmetadata-line [http://perma.cc/K2Q7-S2BW].

109. An ISP need only examine IP addresses (and sometimes domain names) to provide internet service to a subscriber. What's more, web and email metadata are increasingly encrypted, such that an ISP cannot examine them.

110. *See, e.g.*, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 13911 ¶¶ 76, 181-83, 192-93 (2016), *nullified by* S.J. Res. 34, 115th Cong. (2017); *see also* Peter Whoriskey, *Internet Provider Halts Plan To Track, Sell Users' Surfing Data*, WASH. POST (June 25, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/06/24/AR2008062401033.html [http://perma.cc/2TNT-X79G] (describing one cable operator's foray into deep packet inspection and the criticism that followed).

111. *See* United States v. Forrester, 512 F.3d 500, 509-11 (9th Cir. 2008) (email and IP metadata); *In re* Application of the United States for an Order, 396 F. Supp. 2d 45, 48 (D. Mass. 2005) (web and IP metadata); United States v. Allen, 53 M.J. 402, 409 (C.A.A.F. 2000) (web metadata); [Redacted], No. PR/TT [Redacted], at 58-62 (FISA Ct. [date redacted]) (email metadata); *see also In re* Certified Question of Law, No. FISCR 16-01, at 32 (FISA Ct. Rev. Apr. 14, 2016) (analyzing government collection of post-cut-through digits obtained from a telephone carrier). The analysis in the main text is about whether constitutional protections for metadata depend on the government's vantage point when conducting surveillance. That

that metadata – whether phone, web, or email – are knowingly conveyed to *some* third parties. That fact alone is the beginning – and usually the end – of constitutional scrutiny.

The government's preferred doctrinal outcome plausibly draws support from these cases. The underlying principle is, conceivably, that once a person has disclosed metadata to *some* third-party business, it loses all constitutional protection if obtained through electronic means.

iii. Mobile Phone Serial Numbers

Another line of cases that plausibly supports the government's position relates to mobile phone serial numbers. When police seize a mobile phone, they must usually obtain a warrant to search the electronic contents.[112] On occasion, officers have removed the back of the phone in order to read printed serial numbers. Defendants respond by moving to suppress derivative evidence, arguing that opening the phone's case constitutes a Fourth Amendment search.

Courts have so far sided with law enforcement on this issue. Reported opinions conclude that a person does not have a reasonable expectation of privacy in her mobile phone serial numbers, noting that a serial number is non-content identifying information.[113] Removing the phone's case to examine that serial number does not transform the police conduct into a Fourth Amendment search.

Law enforcement hacking, the parallel argument would go, is like removing a mobile phone's cover. The government is merely setting aside the case – a de minimis intrusion, and not even a physical intrusion – to obtain constitutionally unprotected information.

---

analysis presumes that the metadata is functioning solely as metadata (e.g., for routing communications). A related – but distinct – question is whether the metadata and content categories are mutually exclusive, or whether metadata can function both as routing information and as content. On this question, courts have generally held that the metadata and content categories are not mutually exclusive. *See In re* Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 135-39 (3d Cir. 2015) (noting that the distinction between content and metadata is contextual and reviewing opinions).

112. *See* Riley v. California, 134 S. Ct. 2473, 2480-95 (2014) (implicitly holding that police inspection of the electronic contents of a mobile phone constitutes a search while declining to permit warrantless mobile-phone searches incident to arrest).

113. *See, e.g.,* Glenn v. State, No. S17A0858, 2017 WL 4582629, at *5 (Ga. Oct. 16, 2017); State v. Green, 164 So. 3d 331, 344 (La. Ct. App. 2015); *infra* notes 128-131 (additional cases). *But see* State v. Moore, No. 2014-001669, 2017 WL 3723327, at *6-7 (S.C. Ct. App. Aug. 30, 2017) (Lockemy, C.J., concurring in part and dissenting in part) (recognizing in a divided panel decision that police removal and analysis of a mobile phone SIM card constitutes a Fourth Amendment search).

iv. Payment Card Magnetic Stripes

A fourth line of recent cases that plausibly supports the government's position relates to police examination of payment cards. In the typical fact pattern, officers stumble upon a collection of suspicious payment cards during an unrelated traffic stop or arrest. To determine whether the cards are legitimate, the officers will swipe them through a reader and compare their magnetic stripe ("magstripe") data to the information printed on their faces. When the magstripe and printed data are inconsistent, the officers effectuate an arrest for counterfeit access devices.

The federal courts that have considered these scenarios, including three appellate panels, have concluded that a law enforcement magstripe swipe does not constitute a Fourth Amendment search.[114] The opinions reason that the data encoded on a magstripe are constitutionally unprotected because they are account information intended for routine conveyance to third parties (i.e., merchants).

The facts and reasoning of the magstripe cases are arguably analogous to government hacking to recover a network address. A network address is intended for conveyance to third parties, much like the data on a magnetic stripe. Hacking to obtain a network address, the argument goes, is merely a long-distance card swipe.

v. Placing Telephone Calls

A final related scenario, with just a pair of cases on point, involves identifying the owner of a mobile phone. In these fact patterns, a police officer first recovers a suspect's mobile phone from a crime scene. Then, to learn the suspect's identity, the officer places a 911 call and asks the dispatcher for the outbound number.[115]

---

114. *See* United States v. Turner, 839 F.3d 429 (5th Cir. 2016); United States v. DE L'Isle, 825 F.3d 426 (8th Cir. 2016); United States v. Bah, 794 F.3d 617 (6th Cir. 2015); United States v. Alabi, 943 F. Supp. 2d 1201 (D.N.M. 2013), *aff'd*, 597 F. App'x 991 (10th Cir. 2015); United States v. Medina, No. 09-20717-CR, 2009 WL 3669636 (S.D. Fla. Oct. 24, 2009) (Torres, Mag. J.), *adopted in part and rejected in part sub nom.* United States v. Duarte, 2009 WL 3669537 (S.D. Fla. Nov. 4, 2009) (excluding the magstripe evidence on other grounds).

115. *See* State v. Hill, 789 S.E.2d 317 (Ga. Ct. App. 2016); *see also* Cyrus Farivar, *Crook Who Left His Phone at the Scene Has "No Reasonable Expectation of Privacy,"* ARS TECHNICA (June 23, 2016, 3:24 PM), http://arstechnica.com/tech-policy/2016/06/crook-who-left-his-phone-at-the-scene-has-no-reasonable-expectation-of-privacy [http://perma.cc/8FAS-BQQT] (providing a partial transcript of the bench ruling in *United States v. Muller*, No. 2:15-cr-00205-TLN (E.D. Cal. June 23, 2016)).

Both courts to have considered this technique have concluded that it is not a Fourth Amendment search. One opinion emphasized that the suspect had no reasonable expectation of privacy in his telephone number because it was routinely disclosed to third-party businesses for call-routing purposes.[116] It was not of constitutional significance, in the court's view, that the outgoing call was an investigative step by a police officer rather than a voluntary call placed by the cellphone's owner.[117]

Hacking a computer to learn the owner's identity is quite similar to these identifying phone calls. In both scenarios, law enforcement investigators compel a suspect's device to initiate a communication that discloses identifying, non-content information. If placing an identification call to the government from a suspect's seized mobile phone does not implicate the Fourth Amendment, then it is plausible that sending an identifying packet to the government from a suspect's device is also not a constitutional search.

* * *

These five lines of cases do lend support to the government's position. But, critically, it is possible to explain all five lines of cases by applying established Fourth Amendment principles. At most, these cases are consistent with the government's preferred doctrinal outcome – but they hardly compel that outcome.

Beginning with the mobile phone location cases, lower courts are concluding, with increasing frequency, that phone location is protected by the Fourth Amendment[118] – especially when the government causes a suspect's device to generate new location information.[119] Furthermore, five Justices have signaled that they are prepared to rule in favor of constitutional protection for mobile-phone location records.[120] Scholars suggest that the line of cases on which the government's position relies will be sharply limited – if not eliminated – in the

116. *Hill*, 789 S.E.2d at 318-20.

117. *Id.* at 320-21.

118. *See, e.g.*, United States v. Cooper, No. 13-cr-00693-SI-1, 2015 U.S. Dist. LEXIS 25935, at *15-26 (N.D. Cal. Mar. 2, 2015) (concluding that historical cell-site location records can be protected by the Fourth Amendment, and collecting cases and state statutes).

119. *See supra* note 102 (collecting recent cases on cell-site simulators).

120. *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques."); *id.* at 964 (Alito, J., concurring in the judgment) ("I conclude that the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment.").

coming years.[121] In the current term, the Supreme Court is considering *Carpenter v. United States*,[122] and will directly confront whether mobile-phone location data are protected by the Fourth Amendment.

But even assuming that the mobile phone location cases are and will remain good law, those cases are readily explained by the third-party doctrine. Mobile phone location records are classic third-party business records, exempt from Fourth Amendment protection. And even when investigators "ping" a suspect's phone to learn its location, there remains a viable version of the third-party doctrine argument. Mobile phones are designed to facilitate location by carriers, for purposes of providing service, theft tracking, and directing emergency aid. Pinging is nothing more than invoking existing and standard phone functionality that is intentionally made available to the wireless carrier (i.e., a third-party business).

Law enforcement hacking, by contrast, does not involve standard device functionality. Rather, the very purpose is to subvert the device's ordinary operation and extract otherwise inaccessible information. The version of the third-party doctrine that enables warrantless mobile phone tracking has no bearing on government malware.

Turning to the ISP-based surveillance cases, courts have not yet reevaluated those rulings in light of recent Fourth Amendment jurisprudence. Since the *Warshak* opinion in 2010, courts have consistently recognized constitutional privacy protection for communications content held by third-party businesses.[123] To date, no court has grappled with how *Warshak* applies to ISP-based surveillance.[124]

But once again, even assuming that these ISP-based surveillance cases are good law, they can be readily explained under the third-party doctrine and without implicating logical integrity interests. In these cases, the government accomplishes its surveillance via the ISP's equipment, even though the ISP is not the intended recipient of the surveilled data. In other words, the government obtains communications metadata from *some* third-party business. It was not the *specific* third party to whom the suspect had conveyed metadata for processing, but it

121. *See, e.g.*, Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012) ("The concurring opinions in *Jones* raise the intriguing possibility that a five-justice majority of the Supreme Court is ready to endorse a new mosaic theory of Fourth Amendment protection.").

122. 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017).

123. United States v. Warshak, 631 F.3d 266, 283-88 (6th Cir. 2010) (concluding that the Fourth Amendment applies to content stored with a communications service provider).

124. One court has permitted the interception via a telephone carrier of digits dialed after a call has been connected. *See In re* Certified Question of Law, 858 F.3d 591, 604 (FISA Ct. Rev. 2016).

was still *a* third party that consensually received the data – rendering it constitutionally unprotected.[125]

Law enforcement hacking to identify a Tor user, by contrast, does not involve collecting data from *any* third party who is a consensual recipient.[126] That is because, in Tor's design, a user only consensually discloses their IP address to her ISP and an individual Tor server; a user does not otherwise consensually disclose identifiable data to any third party in connection with their online activity.[127] The very purpose of law enforcement hacking is to collect that data not from a third party but from the suspect's *own* electronic device.

The mobile phone serial number cases are also easy to explain. They, too, are of questionable vitality: there are just a handful of reported opinions, and the only federal appellate court to discuss the issue noted that it was a difficult, open question.[128] But even if the cases are correct, they can be readily justified as permissible searches incident to arrest,[129] inventory searches,[130] or perhaps even stop-and-identify practices.[131]

---

125. This version of the third-party doctrine argument is slightly different from the version that plausibly permits warrantless mobile phone location tracking. This version centers on whether the government obtains data via a business that consensually carries the data as a third-party service provider. The version that applies to mobile phone tracking, by comparison, turns on whether the government obtains data via a technical capability that is consensually made available to a third-party service provider. The former argument is fairly similar to how the third-party doctrine usually applies to communications providers, while the latter argument is most similar to cases involving file sharing networks (where the suspect has intentionally enabled certain third-party remote access to their device) or law enforcement deception to gain entry onto private property (here the deception is the police posing as the wireless carrier and the private property is the mobile phone functionality).

126. To be technically precise, the government may learn a suspect Tor user's IP address from communications metadata transmitted by his computer and through his ISP to the government, rather than from directly querying a software interface on the computer and reporting the results. But, in either technical design, government malware is the only reason why the communications metadata emanates from the suspect's computer.

127. *See generally* Dingledine et al., *supra* note 19 (describing Tor).

128. United States v. Green, 698 F.3d 48, 53 (1st Cir. 2012) ("The question . . . whether the . . . retrieval of [the defendant's] IMSI number constituted a search . . . is not, in our view, an easy one.").

129. *See* United States v. Rodriguez, No. 11-205 (JRT/LIB), 2012 WL 73008, at *3-4 (D. Minn. Jan. 10, 2012) (concluding that police inspection of a mobile phone's FCC ID number was permissible as a physical search incident to arrest).

130. *See* United States v. Lowe, No. 2:14-cr-00004-JAD-VCF, 2014 WL 5106053, at *11-12 (D. Nev. Oct. 10, 2014).

131. *See* United States v. Green, No. 09-10183-GAO, 2011 U.S. Dist. LEXIS 157369, at *8-10 (D. Mass. Jan. 11, 2011), aff'd, *Green*, 698 F.3d 48.

Government hacking does not implicate any of these longstanding Fourth Amendment doctrines. There is no arrestee, property to inventory, or suspicious person to identify.

The magstripe opinions can also be explained, in some instances, as permissible searches incident to arrest or inventory searches. There is also a more universal explanation available: the Fourth Amendment's treatment of contraband material. A law enforcement technique that solely indicates the presence or absence of contraband is not a search.[132] When an officer swipes a suspicious card, she only learns that either (a) the magnetic stripe encodes data identical to the face of the card (i.e., the card is not contraband) or (b) the card encodes different data (i.e., the card is contraband). In other words, a magstripe swipe is merely a contraband search.

Government hacking to obtain identifying information, by contrast, does not implicate the Fourth Amendment's exception for contraband. There is nothing inherently unlawful about an IP address.

Finally, the pair of cases in which police placed outbound calls are readily explained by the Fourth Amendment's treatment of abandoned property. In those cases, the suspects abandoned their mobile phones. When a person disposes of his property, he extinguishes his Fourth Amendment privacy interests in the property.[133] Alternatively, those cases may be explained as inventory searches, where police are making a routine effort to catalog the evidence they have obtained.[134]

Law enforcement malware does not involve any abandoned property or property that has already been lawfully seized. In fact, the device that the government hacks often is located in the suspect's own home.

In sum, the government's position—that remotely obtaining data from a device does not constitute a Fourth Amendment search so long as the data are not constitutionally protected—is not frivolous. There is a degree of case law support. But that support is exceedingly thin: every line of cases can be readily explained without accepting the government's position.

---

132. *See, e.g.*, Illinois v. Caballes, 543 U.S. 405, 408-10 (2005) (sniff test by a trained narcotics dog during a vehicle stop is not a Fourth Amendment search); United States v. Jacobsen, 466 U.S. 109, 122-26 (1984) (narcotics field test on powder is not a Fourth Amendment search); United States v. Place, 462 U.S. 696, 706-07 (1983) (sniff test by a trained narcotics dog at an airport is not a Fourth Amendment search).

133. *E.g.*, California v. Hodari D., 499 U.S. 621, 628-29 (1991) (rock of cocaine dropped while fleeing police pursuit); California v. Greenwood, 486 U.S. 35, 39-44 (1988) (garbage placed outside the home); Hester v. United States, 265 U.S. 57, 58-59 (1924) (illegal whiskey bottle abandoned during police pursuit); *see also* Farivar, *supra* note 115.

134. *E.g.*, Illinois v. Lafayette, 462 U.S. 640, 643-48 (1983) (inventory search of an arrestee's bag); South Dakota v. Opperman, 428 U.S. 364, 375-76 (1976) (inventory search of an impounded vehicle).

b. A Better Position: The Fourth Amendment Protects Logical Integrity

A superior rule for the Fourth Amendment and law enforcement hacking holds that any infringement of logical integrity constitutes a Fourth Amendment search. This Section locates support for the rule in the Supreme Court's seminal *Katz v. United States* opinion; the Court's recently articulated concern for electronic devices in *Riley v. California*; lower court cases on cloud service searches; the consent-based underpinnings of the third-party doctrine; and normative considerations. The logical integrity rule has a far stronger basis in doctrine, theory, and policy than the government's preferred outcome.

i. Katz v. United States

The modern history of the Fourth Amendment derives from the recognition that information privacy interests are not coextensive with physical barriers. *Katz* established that a property interest is neither necessary nor sufficient for constitutional privacy protection; to return again to Justice Stewart's famed turn of phrase, the "Fourth Amendment protects people, not places."[135]

The government's proposed rule would draw a sharp distinction between breaches of physical integrity to obtain constitutionally unprotected data and breaches of logical integrity to obtain the same data; the former would necessarily constitute a Fourth Amendment search, while the latter would not. This distinction is inconsistent with *Katz*'s core principle that physical spaces should not be the yardstick for Fourth Amendment interests.

Another principle from *Katz* suggests that any infringement of logical integrity is a Fourth Amendment search. The *Katz* Court explained that constitutional privacy interests are defined by an individual's reasonable expectations of privacy. Conveniently, the contours of a device's logical integrity are typically *also* coextensive with privacy expectations. As discussed in Section I.A.2 above, modern software security is usually implemented via application sandboxing. The very purpose of a sandbox is to conform to and calibrate users' expectations about security and privacy. So, a breach of a device's logical integrity—by breaking out of a software sandbox—is necessarily a Fourth Amendment search under the *Katz* standard.

ii. Riley v. California

The Supreme Court's more recent guidance in *Riley* also favors treating all breaches of logical integrity as Fourth Amendment searches. As many scholars

135. Katz v. United States, 389 U.S. 347, 351 (1967).

and courts have acknowledged, *Riley* demands a higher level of concern when law enforcement officers interact with a suspect's electronic device as opposed to a conventional closed container. As several commenters have put it, *Riley* means that "digital is different."[136]

The government's proposed rule effectively ignores the rationale behind *Riley*. On its account, physically interacting with a device would constitute a search, but remotely accessing the processing and storage of that same device—precisely what caused the Court to sound a privacy alarm in *Riley*—would not implicate the Fourth Amendment.

This Article's proposed rule, by contrast, is entirely consistent with *Riley*. Whether a breach of integrity is physical or logical, law enforcement would be required to comply with Fourth Amendment safeguards.

iii. Cloud Service Searches and United States v. Warshak

In its landmark *Warshak* opinion, the Sixth Circuit reasoned that an email account is the virtual equivalent of a hotel room or an apartment.[137] A breach of the account is a Fourth Amendment search, much like a breach of a physical space. In the years following *Warshak*, other circuits have cited the opinion with approval, and dozens of lower courts have followed the ruling.[138] The Department of Justice implemented *Warshak* as nationwide policy, and the House of Representatives has twice unanimously voted to enact legislation that would codify *Warshak*.[139]

Assuming that *Warshak* was rightly decided as a matter of positive law, which seems beyond question at this stage, and assuming that the physical space analogy is holding rather than dicta, which it certainly appears to be, then the Fourth Amendment necessarily protects the logical integrity of a person's data stored

136. Riley v. California, 134 S. Ct. 2473, 2489-91 (2014) (comparing electronic device searches to physical searches and concluding that the former implicate substantially greater privacy interests); *see also* Jennifer Granick, *SCOTUS & Cell Phone Searches: Digital Is Different*, JUST SECURITY (June 25, 2014), https://www.justsecurity.org/12219/scotus-cell-phone-searches-digital [http://perma.cc/94RH-42EV] (arguing that *Riley* stands for a Fourth Amendment principle of greater protection for electronic information); Orin Kerr, *The Significance of* Riley, WASH. POST: VOLOKH CONSPIRACY (June 25, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/25/the-significance-of-riley [http://perma.cc/Y3G3-W4YB] (providing a similar analysis).

137. United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010).

138. *See supra* note 74 (discussing *Warshak* and its aftermath).

139. *See* Email Privacy Act, H.R. 387, 115th Cong. (2017); Email Privacy Act, H.R. 699, 114th Cong. (2016); H.R. REP. No. 114-528, at 9 (2016) (noting that *Warshak* became DOJ policy in 2013).

with a service provider.[140] If a person can establish a constitutionally protected logical integrity interest in a third-party business's data center, then surely she can establish a logical integrity interest in her own data stored on her own computer at her own home. In other words, accepting the *Warshak* opinion means accepting the logic of logical integrity interests and accepting that government hacking is necessarily a Fourth Amendment search.

iv. The Consent-Based Limiting Principle for Constitutional Information Privacy

The early cases limiting Fourth Amendment information privacy arose from police informants. In *Hoffa v. United States*, the Supreme Court held that there is no Fourth Amendment protection for a suspect's statements to an informant.[141] In *United States v. White*, the Court went a small step further, and concluded that there is no constitutional privacy interest in statements electronically transmitted by an informant.[142]

Hoffa and *White* were followed by a pair of cases involving surveillance via businesses. In *United States v. Miller*, the Court decided that law enforcement access to bank records does not constitute a Fourth Amendment search.[143] In *Smith v. Maryland*, the Court reached the same conclusion for law enforcement access to telephone records.[144]

The final pair of cases limiting information privacy related to physical location. In *United States v. Knotts*, the Court reasoned that there is no Fourth Amendment protection for a person's public movements.[145] The next year, in *United States v. Karo*, the Court found a cognizable information privacy interest in a person's location at home.[146]

Courts and scholars have mixed and matched these six Supreme Court cases that limit Fourth Amendment information privacy into a variety of doctrinal formulations, including the "third-party doctrine," the "metadata doctrine," and the

---

140. *See* United States v. Ackerman, 831 F.3d 1292, 1306 (10th Cir. 2016) (Gorsuch, J.) (discussing the application of *Warshak* and noting that "no one before us disputes that an email is a virtual container").

141. 385 U.S. 293 (1966).

142. 401 U.S. 745 (1971).

143. 425 U.S. 435 (1976).

144. 442 U.S. 735 (1979).

145. 460 U.S. 276 (1983).

146. 468 U.S. 705, 714 (1984) (holding "monitoring of a beeper in a private residence" to be a Fourth Amendment violation).

"public movements doctrine." Whatever the terminology, the underlying principle is the same: the Fourth Amendment does not protect information that a suspect *voluntarily discloses* to a third party or the public, as long as the government obtains the information from the *intended recipient* of the information. As Orin Kerr has explained, the limiting principle of constitutional information privacy is grounded in consent: under current Fourth Amendment doctrine, a person cannot reasonably expect privacy in information that he intentionally discloses, because the recipient of the information could be (functionally) a police informant.[147]

Law enforcement hacking flunks the Fourth Amendment's limiting principle. First, government malware does not involve voluntary disclosure. While law enforcement hacking often begins with a consensual act (the suspect clicks a link or visits a website), the very purpose of hacking is to exceed the scope of that consent, circumvent security and privacy protections, and force a suspect's device to disgorge information.[148] Second, hacking does not involve obtaining information from an intended recipient. The sole reason that the government receives data from the suspect's device is that the government's own software sends the data.

---

147. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 588-90 (2009).

148. *See* Florida v. Jimeno, 500 U.S. 248, 250-52 (1991) (describing the scope of Fourth Amendment consent). Several appellate courts have recognized a "consent once removed" exception to the Fourth Amendment warrant requirement, where initial consent to a law enforcement entry transfers to immediately subsequent law enforcement entry. *See* Callahan v. Millard County, 494 F.3d 891, 895-98 (10th Cir. 2007), *rev'd on other grounds sub nom.* Pearson v. Callahan, 555 U.S. 223 (2009); United States v. Bramble, 103 F.3d 1475, 1478 (9th Cir. 1996); United States v. Akinsanya, 53 F.3d 852, 855-56 (7th Cir. 1995). Whatever the vitality of the consent-once-removed doctrine, it does not provide a basis for warrantless law enforcement hacking. First, a suspect's consent once removed has the same scope as the suspect's initial consent. *See, e.g.*, *Bramble*, 103 F.3d at 1478-79 ("When entering pursuant to the suspect's 'consent once removed,' the additional backup officers are restricted to the scope of the consent originally given. Our holding does not authorize police to go beyond those areas consented to or to conduct general searches without first satisfying the ordinary requirements of consent, a warrant, or exigent circumstances which excuse the failure to obtain a warrant." (citations omitted)). Second, the consent-once-removed exception only allows for a subsequent entry to effectuate a warrantless arrest; any additional warrantless search or seizure must be justified by a separate exception to the Fourth Amendment's warrant requirement. *See, e.g.*, State v. Henry, 627 A.2d 125, 132 (N.J. 1993) (applying the search incident to arrest and protective sweep exceptions).

v. Policy Considerations

There are also policy reasons to favor recognizing Fourth Amendment protection in cases involving remote access to metadata. Imposing an across-the-board warrant requirement for government malware avoids a foreseeable doctrinal morass about when, exactly, the Fourth Amendment kicks in.[149] The alternative would require courts to carefully divvy up a computer's (virtual) innards, holding various parts to be within or outside the scope of constitutional privacy safeguards.[150]

A warrant mandate also increases uniformity and predictability for law enforcement agencies. Rather than haggling with attorneys and scrutinizing local case law, officers can get started right away with drafting affidavits. Uniformity is especially critical for the government's watering hole delivery strategy, where one warrant in one district must be consistent with Fourth Amendment doctrine nationwide.

The limited burden on law enforcement also weighs in favor of a strict warrant requirement. A warrant requirement is not much of a hurdle in the context of government malware.[151] By the time investigators have singled out a target computer system or user, they should have ample factual basis to substantiate probable cause.[152]

Finally, imposing a warrant requirement on all law enforcement hacking avoids a foreseeable Fourth Amendment parade of horribles. The Supreme Court has clearly held that there is no constitutional privacy interest in contraband material.[153] What happens if the government widely distributes malware that only reports back in the presence of unlawful material, such as illegally copied music files? Are we prepared for a society in which, at the press of a button, the government could constitutionally hack and identify millions of Americans

---

149. *Cf.* United States v. Jones, 565 U.S. 400, 411-13 (2012) (articulating a doctrinal preference against "thorny" Fourth Amendment search problems).

150. *Cf.* Riley v. California, 134 S. Ct. 2473, 2493 (2014) (arguing against ambiguous line-drawing exercises for various types of digital files contained on a device).

151. *See* Email from [Redacted] to [Redacted] (Dec. 8, 2004), *in* 1 ELEC. FRONTIER FOUND., *supra* note 93, at 5 ("Until a policy or directive is put in place, [the Data Intercept Technology Unit] has and will support any case that obtains a search warrant. Over the last six months it has not proven to be an obstacle to investigations.").

152. *See* Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 94 MINN. L. REV. 1514, 1535-42 (2010) (arguing that probable cause develops early in online investigations); *see also infra* Section II.B (discussing the application of Fourth Amendment requirements to searches where a particular computer cannot be identified in advance).

153. *See* sources cited *supra* note 132.

who have committed mundane misdemeanors? This is no thought experiment: the technology is straightforward and exists today.[154] Imposing an across-the-board warrant requirement serves as a counterbalance against the vast body of criminal law and as a backstop against sweeping prosecutorial discretion.

* * *

As between the two options for reconciling Fourth Amendment information privacy doctrine, the choice is plain. Courts should end their myopic focus on which data government malware retrieves and acknowledge that government hacking necessarily constitutes a Fourth Amendment search. By design, government malware's exploitation phase breaches the integrity of a device. Thus, regardless of the specific data that government malware reports, agents must presumptively obtain a warrant.

II. RULES FOR MALWARE

This Part continues the positive law inquiry, leveraging the analysis and technical framework from Part I to solve a set of procedural puzzles grounded in the Fourth Amendment, the Federal Rules of Criminal Procedure, the Federal Magistrates Act, and the Electronic Communications Privacy Act. Sections assess when government access becomes a search and presumptively requires a warrant (Section A), how the Fourth Amendment's probable cause and particularity requirements apply (Section B), the proper venue for issuing a warrant (Section C), how long the search lasts (Section D), when and how the government must notify device owners (Section E), and when the government must satisfy heightened super-warrant requirements (Section F). The conclusion of the Part (Section G) advocates for a consistent application of super-warrant requirements to government hacking.

154. An easy technical implementation of this investigative technique would be to generate a set of signatures for known contraband files, then check each file on a hacked device for whether the signature matches. A family of mathematical algorithms dubbed "cryptographic hashing" enables quickly computing these file signatures. *See* Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 43-46 (2006) (arguing that an examination of a seized device for file hashes that match known contraband would not constitute a Fourth Amendment search); *see also* Note, *Data Mining, Dog Sniffs, and the Fourth Amendment*, 128 HARV. L. REV. 691, 705-12 (2014) (discussing a hypothetical "crime-sniffing algorithm").

A. *Initiating a Search*

At what stage of operation does a government malware deployment become a Fourth Amendment search? In some scenarios, the first stage – delivery – will trigger Fourth Amendment safeguards. If government agents sneak into a suspect's home or private office to install malware, for instance, they have unambiguously intruded into a constitutionally protected area.[155] Similarly, if investigators plug a flash drive into a suspect's device, that would constitute a search.[156] In general, though, the delivery phase will not trigger constitutional privacy protections because law enforcement officers have broad discretion to engage in deception.[157] The delivery stage of a phishing attack is roughly akin to tricking a suspect into opening a letter, and the delivery stage of a watering hole attack is approximately equivalent to slipping an insert into a suspect's mail.[158] Neither practice would trigger Fourth Amendment scrutiny.

The exploitation step is more complicated. For decades, courts have struggled to define what constitutes "hacking" into or "unauthorized access" to a computer system. Under the federal Computer Fraud and Abuse Act (CFAA) and parallel state statutes, the judiciary and scholars have developed at least seven distinct substantive tests.[159] While there is no end in sight for debate over the

---

155. *See* Payton v. Riddick, 445 U.S. 573, 586 (1980) (noting that the "physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed") (quoting United States v. U.S. Dist. Court, 407 U.S. 297, 313 (1972)). The government has previously applied for hacking warrants where the delivery stage involves entry into the suspect's home or private office. *E.g.*, United States v. Laurita, No. 8:13CR107, 2016 WL 4179365, at *3 (D. Neb. Aug. 5, 2016) (describing a search warrant that authorized entering a suspect's home and installing malware); Order at 3-6, *In re* Application of the U.S. for an Order Authorizing the Surreptitious Entry into the Premises of Merchant Servs., No. 99-4061 (D.N.J. June 9, 1999) (search warrant allowing surreptitious entry to a suspect's private office to install malware).

156. *See supra* Section I.B.1.

157. *See, e.g.*, United States v. Contreras-Ceballos, 999 F.2d 432, 434-35 (9th Cir. 1993) (reviewing doctrine permitting law enforcement deception to gain entry to a suspect's home). *But see* United States v. Phua, 100 F. Supp. 3d 1040, 1047-52 (D. Nev. 2015) (describing limits on the government's ability to use deception, including where the government manufactures an exigency).

158. Continuing with the mail analogy, while phishing and watering hole delivery techniques are akin to a suspect consensually accepting a deceptive parcel sent by the government, the exploitation and execution steps are more analogous to a robot nonconsensually slipping out of the parcel and roving about the suspect's home.

159. *See* Jonathan Mayer, *The "Narrow" Interpretation of the Computer Fraud and Abuse Act: A User Guide for Applying* United States v. Nosal, 84 GEO. WASH. L. REV. 1644, 1645-46, 1656-57 (2016) (synthesizing substantive standards for authorization to access a computer system or information). The Computer Fraud and Abuse Act explicitly excepts law enforcement inves-

proper scope of computer crime liability, there is one point of consensus: when a person circumvents a technical safeguard on a computer system, that constitutes a violation.[160]

The circumvention test functions as a tidy translation for established Fourth Amendment doctrine. When law enforcement officers break into a home, bypassing physical security measures (like doors and locks), they effectuate a Fourth Amendment search. Similarly, when government agents break into a computer, circumventing technical protections (like sandboxing), they trigger Fourth Amendment safeguards.

This analysis applies beyond government malware that identifies Tor users. As a rule of thumb, government software that actively probes a consumer device will constitute a search. That is because consumer devices, unlike business servers, are usually configured to be private.[161] When government software is merely responding to an ordinary request from a consumer device, by contrast – such as when a person visits a government website – that will rarely constitute a Fourth Amendment search.

There are exceptions to this rule, to be sure. Consumer devices can advertise information to the public, such as on a peer-to-peer file-sharing network. When government software communicates with a consumer device under those circumstances, there plainly is no breach of physical or logical integrity. Law enforcement may obtain data without first seeking a warrant.[162]

---

tigations from its regulatory scheme. 18 U.S.C. § 1030(f) (2012) ("This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.").

160. *See* Mayer, *supra* note 159, at 1656-57, 1662.

161. When the government remotely probes a business server, much more difficult line-drawing questions can arise. While investigating an online black market, for instance, federal investigators may have engaged in borderline hacking conduct. *See* Nik Cubrilovic, *Analyzing the FBI's Explanation of How They Located Silk Road*, NEW WEB ORD. (Sept. 7, 2014), https://www.nikcub.com/posts/analyzing-fbi-explanation-silk-road [http://perma.cc/E3K3-4XPX] (collecting and technically analyzing government filings associated with locating the black market server). Some remote investigative practices involving business servers do remain easily identifiable as searches, such as entering a user's cloud service account without their permission. *See* Memorandum from David Bitkower, *supra* note 92, at 5 (offering a government hacking scenario where investigators cannot serve a Stored Communications Act warrant on a service provider, so they log into the suspect's account themselves).

162. Courts have, for instance, consistently concluded that government investigators may explore public file-sharing services without triggering Fourth Amendment safeguards. *See, e.g.*, United States v. Hill, 750 F.3d 982, 986 (8th Cir. 2014); United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008); United States v. Perrine, 518 F.3d 1196, 1205 (10th Cir. 2008); *see also* United States v. King, 509 F.3d 1338, 1341-42 (11th Cir. 2007) (finding no search when the government monitored files shared on a shared residential network on a military base). An

Critically, this exemption for advertised data only applies to information made available on *public* networks. If the police obtain advertised data by intruding into a private network—even an unprotected wireless network—they are conducting a search and must usually obtain a warrant.[163] Moreover, if officers intercept advertised data on a private network in real time, they are operating a wiretap and must obtain a super-warrant.[164]

Another (possible) exception of government remote access that does not constitute a search is when the government activates preexisting device functionality that is partially controlled by a third-party business. For example, as discussed earlier, wireless carriers have the capability to remotely enable location reporting from a subscriber's device.[165] This functionality is required on mobile phones, does not involve bypassing any security safeguards, does not include delivering proprietary government software, and does not require entering into any user storage area. But this capability is reserved for extraordinary circumstances, assuredly runs counter to a device user's privacy expectations, and involves tampering with device configuration solely for the government's benefit.[166]

Reasonable minds can disagree on how to apply the circumvention test (or other computer crime tests) in this scenario, and whether these facts should be considered a Fourth Amendment search or an instance of malware. Whatever the resolution, this much is certain: only a small subset of device functionality is remotely available to third parties. These fact patterns are readily distinguishable from most configurations of government malware.

---

early interagency report on computer searches also recognized a distinction between publicly and privately advertised data. U.S. DEP'T OF JUSTICE, ONLINE INVESTIGATIONS WORKING GRP., *supra* note 96, at 20 (suggesting that using the public Unix "finger" command to collect identifying information would not constitute a search, but "exploiting design flaws" to collect the same information would be a search).

163. *See* United States v. Ahrndt, No. 3:08-CR-00468-KI, 2013 WL 179326, at *6-8 (D. Or. Jan. 17, 2013) (invalidating the warrantless search of an unprotected wireless network). In some scenarios, the police may be able to obtain consent from a person with authorized access to the private network. *See* United States v. Sawyer, 786 F. Supp. 2d 1352, 1355-57 (N.D. Ohio 2011).

164. *See* Joffe v. Google, Inc., 746 F.3d 920, 926-36 (9th Cir. 2013) (applying the Wiretap Act to real-time content interception from unprotected wireless networks).

165. *See* FCC Wireless E911 Location Accuracy Requirements, 80 Fed. Reg. 11,806 (Mar. 4, 2015) (to be codified at 47 C.F.R. pt. 20) (discussing the location capabilities of mobile phones and setting new accuracy requirements).

166. *Cf. In re* U.S. Order Authorizing Roving Interception, 349 F.3d 1132, 1133-35 (9th Cir. 2003) (applying the Wiretap Act to remote FBI activation of a car's built-in microphone using theft-tracking functionality).

A third possible exception worth mentioning, since it has been raised by both FBI agents and the Advisory Committee on Rules of Criminal Procedure, is deployment of malware against computer trespassers.[167] (In policy circles, this practice is often dubbed "hack back.") Courts have held that intentional trespassers on real property may not be entitled to Fourth Amendment protection for their personal property.[168] Similarly, the Wiretap Act allows for warrantless surveillance of communications to or from a computer trespasser, so long as the owner of the attacked computer system consents.[169] The recent Cybersecurity Information Sharing Act expanded that permission, such that network and system providers can now monitor all computer trespasser activity that transits their networks or systems.[170]

Courts should decline to recognize a trespasser exception for government malware. For starters, reliance on the physical trespass analogy is factually flawed. A hacker has in no way placed the entirety of her own device "into" the system that they are hacking. Rather, she has selectively sent data to (and received data from) a victim computer.

---

167. *See* Advisory Comm. on Rules of Criminal Procedure, *Criminal Rules Meeting*, JUD. CONF. U.S. 10 (Apr. 7-8, 2014), http://www.uscourts.gov/rules-policies/archives/meeting-minutes/advisory-committee-rules-criminal-procedure-april-2014 [http://perma.cc/7GNJ-MFRP]; Email from [Redacted] to [Redacted] (July 2, 2007, 10:52 AM), *in* 8 ELEC. FRONTIER FOUND., CIPAV FOIA RELEASE 29, https://www.eff.org/files/filenode/cipav/fbi_cipav-08.pdf [http://perma.cc/8TDK-C2W5] ("It is just not well settled in the law that we can rely on the trespasser exception to the search requirement.").

168. *See* Luke M. Milligan, Note, *The Fourth Amendment Rights of Trespassers: Searching for the Legitimacy of the Government-Notification Doctrine*, 50 EMORY L.J. 1357, 1367-74 (2001) (summarizing the state of Fourth Amendment doctrine involving physical trespassers).

169. *See* 18 U.S.C. §§ 2510(21) & 2511(2)(i) (2012); Comput. Crime & Intellectual Prop. Section, Criminal Div., *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, U.S. DEP'T JUST. 177-79 (2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf [http://perma.cc/3ZLW-QYQJ] (explaining the computer trespasser exception to the Wiretap Act).

170. Cybersecurity Information Sharing Act, Pub. L. No. 114-113, § 104, 129 Stat. 2936, 2940-41 (2015) (codified at 6 U.S.C. § 1503 (Supp. III 2016)).

Furthermore, the physical trespass cases involve temporarily abandoned personal property.[171] And even in those fact patterns, courts have sometimes recognized Fourth Amendment protections.[172] A hacker has not, in any sense, abandoned the integrity or contents of her computer. With high probability, in fact, the computer remains at the hacker's home or on her person.

A direct application of the *Katz* test also cuts against recognizing a trespasser exception. A hacker has not manifested a diminished expectation of privacy in her *own* computer by breaking into *someone else's* computer.[173] Using personal property in the commission of a crime does not, by itself, negate Fourth Amendment protection. (If the law were otherwise, the unbroken line of closed-container cases would be erroneous.)

Finally, the Supreme Court's recent guidance in *Riley* disfavors a trespasser exception. Modern technology contains data of extraordinary volume, duration, pervasiveness, and sensitivity.[174] That recognition weighs heavily in favor of a warrant requirement. A trespasser exception would allow the government to "hack back" and obtain a wealth of information, much of it not immediately related to defending the computer system under attack.[175]

Assuming that courts reject a trespasser exception, the resulting rules are straightforward. With a victim's consent, investigators may intercept information sent to or received by a hacker[176] and may monitor data advertised by the

---

171. If a person has a closed container under his or her immediate control, the Fourth Amendment applies. *See* Oliver v. United States, 466 U.S. 170, 179 n.10 (1984) (noting that, even in an entirely public area, Fourth Amendment protection remains for "effects upon the person").

172. *See, e.g.*, State v. Mooney, 588 A.2d 145, 152-61 (Conn. 1991) (concluding that a trespasser had a reasonable expectation of privacy in a sealed duffel bag and cardboard box that he had abandoned).

173. *Cf.* Sam Zeitlin, Note, *Botnet Takedowns and the Fourth Amendment*, 90 N.Y.U. L. REV. 746, 770-77 (2015) (concluding that if the government obtains information from a compromised "zombie" computer that is part of a "botnet," it is conducting a Fourth Amendment search). If anything, it seems reasonably likely that a hacker would have installed additional security precautions, developing a *stronger* argument for a reasonable expectation of privacy.

174. *See* Riley v. California, 134 S. Ct. 2473, 2488-91 (2014) (discussing ways in which the search of a mobile phone is far more intrusive than a physical search).

175. A narrower trespasser exception, allowing the government solely to take steps to prevent an attack or identify the perpetrator, would mitigate this concern. But a narrower exception would have no doctrinal basis, and would require courts to rigorously parse and review each and every category of information that the government obtained.

176. *See* 18 U.S.C. § 2511(2)(i) (2012) (allowing communications content interception against a computer trespasser, with a victim's consent).

hacker on the victim's network.[177] But the moment investigators break into the hacker's computer, they are conducting a search and must ordinarily obtain a warrant.[178]

B. Probable Cause and Particularity

The Fourth Amendment imposes two substantive constraints on a search warrant application: officers must demonstrate probable cause that they will find evidence of a crime, and they must describe that evidence with particularity.[179] These two requirements are deeply intertwined: particularity determines the scope of probable cause, linking it to a specific offense and type of evidence.

Courts are already struggling with how probable cause and particularity apply to the *information* that government agents collect from a suspect's device or

---

177. *See* United States v. Stanley, 753 F.3d 114, 119-24 (3d Cir. 2014) (holding that a network trespasser does not have a Fourth Amendment interest in his or her network configuration as exposed to the victim's network, but rejecting the argument that all information associated with the trespasser is exempt from protection).

178. As with all Fourth Amendment searches, exigent circumstances may excuse the warrant requirement. The Supreme Court has noted that these are highly fact-specific determinations, and require extraordinary justification. *See Riley*, 134 S. Ct. at 2494 (listing bomb detonation and child abduction as hypothetical exigencies where a warrantless mobile phone search might be permissible). The rationale most likely to be applicable to computer trespassers is destruction of evidence, since most electronic attacks do not implicate human life or safety. *See* Kentucky v. King, 563 U.S. 452, 460 (2011) (noting various exigencies that excuse a search warrant). In order for that justification to apply, though, investigators must have reasonable grounds to believe that the hacker is destroying evidence in his or her own computer system. *See* Ker v. California, 374 U.S. 23, 57 (1963) (Brennan, J., concurring) ("Our decisions in related contexts have held that ambiguous conduct cannot form the basis for a belief of the officers that an escape or the destruction of evidence is being attempted."). While it is conceivable that some hackers will satisfy this standard – for instance, by issuing specific taunts – investigators will rarely have sufficient indicia that a hacker plans to purge data from his or her *own* computer. *See* United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *4 (W.D. Wash. May 23, 2001) (concluding in dicta that an exigency justified the warrantless remote copying of a hacking group's data, because the FBI had just arrested two of the hackers and co-conspirators could delete the data). What's more, even if an exigency justifies warrantless remote copying of data, investigators will usually have time to obtain a warrant authorizing examination of the data. *See id.* (noting that investigators obtained a warrant before examining the remotely-seized hacker data).

179. To be precise, a search warrant can also be directed at the fruits or instrumentalities of a crime. *See* Warden v. Hayden, 387 U.S. 294, 300-10 (1967). I focus on evidentiary searches because that is the typical deployment for government malware.

cloud service account. Some courts have required ex ante search protocols, delineating particular pockets of stored data and methods for examining them.[180] Others have allowed broad discretion for investigators, checked solely by ex post suppression motions.[181] In the author's view, given the extraordinary quantity and sensitivity of data stored in electronic devices and the haziness of ex post suppression practice, ex ante restrictions are the better approach.

Law enforcement malware poses these same general problems, and introduces one more: the government may not know which *device* it is hacking. When deploying identification malware, the very purpose is to discover a computer's location and owner. The result is a seeming chicken-and-egg problem: how can investigators describe, with particularity, the very electronic device that they are attempting to discover?

The solution lies in the doctrine of "anticipatory" warrants.[182] Courts have long allowed for law enforcement searches and arrests subject to defined conditions that trigger the warrant's execution.[183] The notion is that courts can identify facts in advance that are likely to occur and that would satisfy probable cause

---

180. *See, e.g.*, United States v. Winn, 79 F. Supp. 3d 904, 918-22 (S.D. Ill. 2015) (invalidating a smartphone search warrant that covered "any or all files contained on said phone" as insufficiently particularized); *In re* [Redacted]@gmail.com, 62. F. Supp. 3d 1100, 1104 (N.D. Cal. 2014) (suggesting that, at minimum, the government must identify date restrictions and commit to returning or destroying relevant evidence in a cloud service search); *In re* Search of Info. Associated with [Redacted]@mac.com, 25 F. Supp. 3d 1, 7-9 (D.D.C. 2014) (calling for online services to prescreen information made available to the government, according to specific times, keywords, parties, or other filtering criteria).

181. *See, e.g.*, *In re* a Warrant for xxxxxxx@gmail.com, 33 F. Supp. 3d 386, 396-401 (S.D.N.Y. 2014) (holding that, in general, ex ante protocols for data searches are not required to satisfy the Fourth Amendment's particularity standard).

182. Anticipatory warrants offer a comprehensive and coherent constitutional basis for identification malware. There are, to be sure, related lines of doctrine that could also be used to justify identification-malware warrants. Courts have long permitted location-tracking warrants, even though at the time of issuance officers do not know where the suspect will travel. *See* United States v. Karo, 468 U.S. 705, 718 (1984). More recently, courts have allowed DNA-based "John Doe" arrest warrants, where officers do not know the suspect's identity at the time of issuance. *See* People v. Robinson, 224 P.3d 55, 71-76 (Cal. 2010).

183. *See* United States v. Grubbs, 547 U.S. 90, 96 (2006) ("Anticipatory warrants are, therefore, no different in principle from ordinary warrants. They require the magistrate to determine (1) that it is *now probable* that (2) contraband, evidence of a crime, or a fugitive *will be* on the described premises (3) when the warrant is executed."); United States v. Garcia, 882 F.2d 699, 702-04 (2d Cir. 1989) (reviewing the doctrine, policy, and precedent that support anticipatory warrants).

and particularity once they do occur.[184] Government agents then wait for the specified triggering conditions and execute their warrant.

Controlled package delivery is the quintessential example of an anticipatory warrant.[185] Courts have consistently upheld search and arrest warrants conditioned upon receipt of a contraband parcel. In these scenarios, officers do not necessarily know in advance when the package will be accepted. They may not even know who will receive the package or where it will be delivered.[186] But it is likely that someone will accept the parcel, and accepting the parcel is a sufficient triggering condition to establish probable cause and particularity to both search the place of delivery and arrest the recipient.

Wiretaps are another established area of permissible anticipatory searches.[187] When seeking a "roving" super-warrant, investigators do not know in advance which places they will bug or which phone lines they will tap.[188] Courts have nevertheless sustained these investigatory practices, emphasizing that the touchstone of the Fourth Amendment is reasonable particularity, not exacting precision.[189]

---

184. *See Grubbs*, 547 U.S. at 96-97 (explaining that an anticipatory warrant requires probable cause both with respect to the triggering condition occurring and to finding evidence once the triggering condition is satisfied). In a controlled-delivery scenario, probable cause with respect to the triggering condition is easily satisfied – packages are usually delivered to their intended destination and recipient.

185. *See Garcia*, 882 F.2d at 702-03 (collecting cases); Joshua D. Poyer, Note, United States v. Miggins*: A Survey of Anticipatory Search Warrants and the Need for Uniformity Among the Circuits*, 58 U. MIAMI L. REV. 701, 745-49 (2004) (noting variations in the requirements among circuits).

186. In the usual controlled-delivery fact pattern, investigators at least know the intended recipient and destination for a package. With a malware search, by contrast, officers cannot provide a name or address in advance. While that sort of ex ante ambiguity is rare in a controlled delivery, it has come up, and courts have sustained anticipatory warrants for unspecified addresses and individuals. *See* People v. Bui, 885 N.E.2d 506, 517-22 (Ill. App. Ct. 2008) (sustaining a controlled-delivery search warrant for "any other location" where a package was taken); State v. Morris, 668 P.2d 857, 861-63 (Alaska Ct. App. 1983) (sustaining a controlled-delivery search warrant for "whoever picks up said package" and "wherever the described package is taken").

187. *See Grubbs*, 547 U.S. at 95-96 (noting that wiretap super-warrants are a type of anticipatory warrant).

188. *See* 18 U.S.C. § 2518(11) (2012) (laying out procedures for roving wiretaps and bugs).

189. *See, e.g.*, United States v. Bianco, 998 F.2d 1112, 1122-25 (2d Cir. 1993) (roving bug); United States v. Petti, 973 F.2d 1441, 1443-45 (9th Cir. 1992) (roving wiretap); *see also Grubbs*, 547 U.S. at 97 ("The Fourth Amendment, however, does not set forth some general 'particularity requirement.' It specifies only two matters that must be 'particularly describ[ed]' in the warrant: 'the place to be searched' and 'the persons or things to be seized.'").

Government hacking follows the same principles as a controlled delivery or a roving wiretap. Agents may not know in advance the exact computer that they are breaching. But they can articulate a conditional set of facts to ensure a fair chance that their malware will be delivered and that its recipient will be a computer system that satisfies probable cause and particularity.

One possible malware trigger is affirmative conduct by a suspect. The FBI's "phishing" attack in the Timberline case is a good example.[190] The target was actively using his social media account, so it was likely that an FBI message would be read. And, given the target's apparent ego, it was very likely that he would click the FBI's bogus news link. Whoever first clicked that link was likely to be the person sending bomb threats, because he had demonstrated control over the social media account. And it was likely that his computer contained evidence of his crimes and identifying information. In more precise Fourth Amendment terminology: there was probable cause that the FBI's malware would be delivered to a particular computer, and there was probable cause that particular criminal evidence would be recovered from that computer.

This phishing approach is not foolproof, to be sure. The government must make sure it delivers malware to the right account. On at least one occasion, FBI agents mistakenly requested a warrant to send malware to the wrong email address.[191] Investigators must also take precautions to limit the likelihood of hacking innocent users; given that links can easily be forwarded or indexed by a search engine, probable cause will quickly dissipate after a phishing attempt.[192] Restricting malware delivery to the first device to visit the phishing link, for instance, might be appropriate. But, in general, using phishing as an anticipatory warrant condition is a constitutionally sound investigative strategy.

Another possible approach to anticipatory warrants is conditioning malware delivery on when the target visits a specific webpage. On at least two occasions,

190. *See supra* notes 2-29 and accompanying text.

191. Third Amended Application for a Search Warrant, *supra* note 37, at 3.

192. *See* Memorandum from Nathan F. Wessler et al., Speech, Privacy & Tech. Project, Am. Civil Liberties Union, to Members of the Advisory Comm. on Criminal Rules 13-14 (Apr. 4, 2014) (on file with author) (describing ways in which a government phishing attack could reach innocent parties).

the FBI has seized an online service and sent identification malware to *all* visitors.[193] This type of watering hole attack has proven exceedingly controversial, since it can involve hacking thousands of users under just one search warrant.[194]

Using a watering hole trigger for government malware can sometimes be constitutionally sustainable. Authorizing multiple searches under one warrant is no issue: courts have consistently permitted that practice.[195] A warrant under the Fourth Amendment requires valid judicial determinations, not formally formatted paperwork.[196]

The challenge is establishing probable cause of a crime and describing evidence with particularity based solely on a visit to a webpage. It is only possible to make that determination in cases involving child pornography, because the criminal statutes on child pornography are exceptionally broad and because the speech protections for child pornography are exceptionally limited. Possessing information, or attempting to possess information, is rarely itself a crime. Child pornography is unique: merely possessing it or attempting to possess it is criminal, and the First Amendment allows for this broad criminalization.[197]

From a Fourth Amendment perspective, then, if a user visits a semi-private website that is exclusively dedicated to distributing child pornography, there is probable cause to believe that the user has committed a crime (attempted possession), and that the user's particular computer contains particular evidence of

---

193. *Application for "Bulletin Board A" Search Warrant*, *supra* note 41, at 30 ("I request authority to use the NIT to investigate: (1) any user who accesses any page in the 'Images' section of 'Bulletin Board A' . . . ."); Poulsen, *supra* note 42.

194. *See* Memorandum from Nathan F. Wessler et al., *supra* note 192, at 14-15 (criticizing watering hole techniques).

195. *See* M.C. Dransfield, Annotation, *Propriety and Legality of Issuing Only One Search Warrant To Search More than One Place or Premises Occupied by Same Person*, 31 A.L.R.2d 864 (1953) (collecting cases that have permitted searches of multiple locations with a single warrant).

196. *See, e.g.*, United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *18-19 (D. Ariz. May 8, 2013) (explaining that a warrant authorizing electronic surveillance need not be a "model of clarity," and need only satisfy the Fourth Amendment's basic requirements of a neutral and disinterested magistrate, probable cause, and particularity). As a matter of policy, greater clarity in warrant documentation is certainly preferable, but not a constitutional requirement.

197. 18 U.S.C. §§ 2251, 2252, 2252A (2012); United States v. Williams, 533 U.S. 285, 292-304 (2008) (holding that an offer to provide or request to receive child pornography is categorically unprotected by the First Amendment); New York v. Ferber, 458 U.S. 747, 753-74 (1982) (holding that the possession of child pornography is categorically unprotected by the First Amendment).

that crime (identifying information). The government relies upon this very reasoning in its watering hole deployments.[198]

Most websites, though, serve multiple purposes and are open to the public. The government may need to impose extra conditions on its watering hole delivery to ensure probable cause. Merely visiting the site is insufficient; waiting for a user to log in or send a private message, for instance, would offer firmer footing. Prior watering hole warrants have involved each of these conditions.[199]

As with phishing, it appears that the government does not always correctly execute this strategy for developing probable cause. In a highly publicized episode, the FBI appears to have seized a set of webservers and deployed malware to anyone visiting any of the hosted websites.[200] Some of the websites were dedicated to child pornography, such that probable cause may have existed for each visitor to those sites. But many of the websites hosted information that was not criminal and could not be criminal under the First Amendment, rendering the FBI's hacking of visitors constitutionally infirm.

C. Venue

When investigators intend to apply for a hacking warrant, which courthouse should they go to? Both the Federal Rules of Criminal Procedure and the Federal Magistrates Act establish geographic limitations on which court may issue a hacking warrant.

The venue provisions in Rule 41 that predate the recent rise in government hacking are reasonably clear. A federal magistrate judge has authority to issue search warrants for property within her district.[201] A magistrate can also issue a warrant for property outside her district, but only in exceptional circumstances. Until recently, those circumstances were: property currently within the district that might move outside the district, terrorism investigations, tracking device

---

198. *See, e.g.*, *Application for "Bulletin Board A" Search Warrant*, *supra* note 41, at 30.

199. Affidavit of FBI Special Agent John Robertson in Support of Application for a Search Warrant at 12, No. 1:15-mj-00534-VVP (E.D.N.Y. June 10, 2015) (describing a warrant that authorized malware delivery from a seized child pornography website "each time any user or administrator logged [in]"); *Application for "Bulletin Board A" Search Warrant*, *supra* note 41, at 30 ("I request authority to use the NIT to investigate: . . . (2) any user who sends or views a private message on 'Bulletin Board A' during the period of this authorization.").

200. Poulsen, *supra* note 42.

201. FED. R. CRIM. P. 41(b)(1); *see* Owsley, *supra* note 28, at 320-23 (reviewing applicable venue provisions).

installation within the district, and crimes committed on certain federal property.[202] Law enforcement hacking across state lines usually was not covered—even when the government had no way of knowing the target device's location, such as when the suspect was a Tor user.[203]

The Department of Justice, understandably, sought an amendment to Rule 41 that would permit extra-district hacking warrants where the location of the search is unknown.[204] The amendment became effective on December 1, 2016, and it resolves the venue puzzle under the Federal Rules of Criminal Procedure.[205] If the government knows the location of the device it is hacking, investigators usually must apply to a judge in the district where the device is located.[206] If the government does not know the location of the device, because it has been "concealed through technological means," investigators can apply to a judge in "any district where activities related to [the] crime may have occurred."[207]

---

202. FED. R. CRIM. P. 41(b)(2)-(5).

203. The previous result under Rule 41 was that when the government knew which computer it was hacking, investigators would apply to a magistrate judge in the district where the computer was located. When the government was hacking a computer in a terrorism-related case, a magistrate in any district would suffice. But when the government wanted to hack a computer and did not know where the computer was located (e.g., when investigating a Tor user), a substantial majority of lower courts rightly concluded that there was no exceptional Rule 41 venue provision—textually or in principle. *See, e.g.*, United States v. Adams, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *10 (M.D. Fla. Aug. 10, 2016); United States v. Werdene, No. 15-434, 2016 WL 3002376, at *11 (E.D. Pa. May 18, 2016). *But see* United States v. Laurita, No. 8:13CR107, 2016 WL 4179365, at *7 (D. Neb. Aug. 5, 2016); United States v. Eure, No. 2:16CR43, 2016 WL 4059663, at *4 (E.D. Va. July 28, 2016). There was a plausible argument that District Court judges retained authority to issue these types of warrants under 18 U.S.C. § 3103, regardless of Rule 41.

204. FED. R. CRIM. P. 41(b)(6). *See* Daskal, *supra* note 29, at 355-59 (reviewing the proposed amendments); Lerner, *supra* note 28 (similar); *see also* Ghappour, *supra* note 28, at 1080-81 (criticizing the proposed amendments). The discussion above centers on FED. R. CRIM. P. 41(b)(6)(A), because it resolved an outstanding and difficult venue issue in malware-based investigations. The new amendment also added FED. R. CRIM. P. 41(b)(6)(B), which streamlines the warrant process for remotely accessing compromised devices in multi-district investigations.

205. *See* FED. R. CRIM. P. 41 advisory committee's notes.

206. The extra-territoriality provision for terrorism investigations still applies to law enforcement hacking. If the government is investigating "domestic terrorism or international terrorism," it can apply for a hacking warrant in "any district in which activities related to the terrorism may have occurred." FED. R. CRIM. P. 41(b)(3).

207. FED. R. CRIM. P. 41(b)(6)(A).

Judicial rules are not the only venue constraints on warrant issuance.[208] United States Magistrate Judges are Article I judges, invested with only the powers that Congress has provided. And the Federal Magistrates Act includes an express geographic restriction. A magistrate possesses "all powers and duties conferred or imposed . . . by law or by the Rules of Criminal Procedure for the United States District Courts."[209] But a magistrate only has those powers or duties "within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere *as authorized by law*."[210] In other words, in a plain reading of the statutory text, the Federal Rules of Criminal Procedure can only create new powers and duties for magistrate judges *within their district*. The Federal Rules cannot create extra-district powers or duties.

Warrants that authorize law enforcement hacking often involve searches of extra-district property. The question under the Federal Magistrates Act is: are those searches an exercise of extra-district power, such that they must be authorized by statute rather than rule?

Recent congressional experience suggests that the answer is yes. In every instance where magistrate judges have received new authority to issue warrants for extra-district persons or property, the change has only occurred after legislative authorization.[211] The Rule 41 provision allowing extra-district warrants in terrorism investigations was a component of the USA PATRIOT Act, which expressly empowered magistrates.[212] The provision allowing extra-district tracking device operation followed the Electronic Communications Privacy Act, which also expressly empowered courts.[213] The provision allowing extra-district

---

208. *See* United States v. Krueger, 809 F.3d 1109, 1117-26 (10th Cir. 2015) (Gorsuch, J., concurring) (detailing how the Federal Magistrates Act imposes warrant venue provisions); *see also* United States v. Arterbury, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091, at *7-8 (N.D. Okla. Apr. 25, 2016) (concluding that a magistrate's issuance of a warrant to hack Tor users violated the Federal Magistrates Act).

209. 28 U.S.C. § 636(a)(1) (2012).

210. 28 U.S.C. § 636(a) (2012) (emphasis added).

211. Relatedly, in the instance where magistrate judges received new authority to preside outside their district, that was also authorized by legislation. The statutory authority for magistrates to operate "at other places where that court may function" was added in 2005, as a response to the displacement of federal courts following Hurricane Katrina. *See Krueger*, 809 F.3d at 1121 (Gorsuch, J., concurring).

212. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, § 219, 115 Stat. 272, 291. While the provision addressing extra-district search warrants is framed as an amendment to Rule 41, it is nevertheless a *congressional* enactment.

213. Electronic Communications Privacy Act of 1986 § 108(a), 18 U.S.C. § 3117 (2012).

search warrants for federal lands has a basis in the statute providing a default venue for crimes committed on federal lands.[214] Extra-district warrants for stored communications content are solely established by statute, rather than a provision of the rule.[215]

While the issue is a close one, in the author's view, the better position is that magistrate judges currently lack statutory authority to issue extra-district hacking warrants. Thankfully, there is a straightforward workaround for the issue. District court judges are also empowered to issue search warrants, and they are not subject to the constraints of the Federal Magistrates Act.[216] When the government intends to search a computer but does not know the computer's location, it can (and must) submit a warrant application to a district court judge rather than a magistrate judge.

D. Search Duration

When law enforcement agents exploit a device, they conduct a Fourth Amendment search and they presumptively must obtain a warrant. But how long does the search last and, consequently, what time period must the warrant cover?

The view of the Department of Justice appears to be that, to the extent hacking constitutes a search, the search occurs solely at the moment of exploitation. In the Timberline case, for instance, investigators combined a search warrant with a lesser pen/trap order. The search warrant was valid for only 10 days, and covered installation of the malware; the pen/trap order was valid for 60 days, and covered subsequent execution by and reporting from the malware.[217]

The government's approach is not consistent with Fourth Amendment principles. As discussed in Part I, law enforcement hacking is a Fourth Amendment search because the government breaches the logical integrity of an electronic device. That breach of integrity first occurs at the exploitation stage, when law enforcement agents circumvent technical protections on the device. But that breach

---

214. 18 U.S.C. § 3238 (2012).

215. 18 U.S.C. § 2703 (2012).

216. District court judges are authorized to issue search warrants under 18 U.S.C. § 3102 (2012), and the Federal Rules of Criminal Procedure expressly provide district court judges with all of the powers of magistrate judges. FED. R. CRIM. P. 1(c). Courts have also understood that Rule 41 regulates warrants issued by district court judges, even though the text of the rule references magistrates. *See, e.g.*, United States v. Golson, 743 F.3d 44, 51-53 (3d Cir. 2014); United States v. Glover, 736 F.3d 509, 515 (D.C. Cir. 2013).

217. Application and Affidavit for Search Warrant, *supra* note 4, at 13-15.

of integrity *continues* throughout the execution stage, so long as the government malware is resident and running on the suspect's device.

Drawing a parallel to physical searches is instructive. When the government compromises physical integrity to conduct a search, such as by installing a location tracker on a car[218] or an electronic device in a home,[219] courts have unhesitatingly concluded that an ongoing warrant is required. A rule allowing for continued malware operation without a warrant would represent an unsupported distinction between physical and electronic integrity.

Case law related to wiretapping also favors an ongoing warrant. The Supreme Court has emphasized that interception of communications requires a continuously valid super-warrant,[220] and the Wiretap Act imposes ongoing substantive requirements.[221] A rule permitting continued computer hacking with a one-time judicial determination would create unjustified inconsistency between the treatment of malware and of other means of collecting information.

The doctrinal result is that there is a Fourth Amendment search throughout the duration of malware operation. The government must obtain a warrant that is continuously valid from exploitation through execution. A pen/trap order does not suffice, because it does not satisfy the Fourth Amendment's probable cause and particularity requirements.[222]

The temporal regulation of law enforcement hacking under the Federal Rules of Criminal Procedure is straightforward. Under the current Rule 41, a warrant

---

218. *See, e.g.*, United States v. Katzin, 732 F.3d 187, 198 (3d Cir. 2013) ("We thus have no hesitation in holding that the police must obtain a warrant prior to attaching a GPS device on a vehicle, thereby undertaking a search that the Supreme Court has compared to 'a constable's concealing himself in the target's coach in order to track its movements.'" (quoting United States v. Jones, 565 U.S. 400, 406 n.3 (2012))).

219. *See, e.g.*, Silverman v. United States, 365 U.S. 505, 511-12 (1961) ("This Court has never held that a federal officer may without warrant and without consent physically entrench into a man's office or home, there secretly observe or listen, and relate at the man's subsequent criminal trial what was seen or heard.").

220. Berger v. New York, 388 U.S. 41, 59 (1967) ("[A]uthorization of eavesdropping for a two-month period is the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause.").

221. 18 U.S.C. § 2518(5) ("No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization . . . .").

222. *Compare* 18 U.S.C. § 3122 (2012) (requiring only a self-certification of relevance to substantiate a pen/trap order), *with* U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

must be executed within fourteen days of issuance.[223] The government, then, has fourteen days to hack a device and collect data from it. After fourteen days, the government must either obtain a new warrant or disable its malware.[224]

In at least five additional cases, the government has failed to adhere to this simple formulation. A 2012 warrant in the District of Colorado authorized malware operation for fourteen days after installation (whenever that occurred), rather than fourteen days after warrant issuance.[225] The accompanying affidavit suggested treating installation as a warrant triggering condition, allowing for extended time.[226] But that reasoning misunderstands the doctrine of anticipatory warrants, which allows for conditional search *execution*; the warrant is still *issued*, and the Rule 41 clock starts running, once it is signed by the reviewing judge.[227]

In a trio of District of Nebraska warrants that same year, authorizing the Operation Torpedo investigation, the FBI obtained approval for computer searches with two distinct time periods. Agents had fourteen days to install malware delivery software onto a webserver that they had seized, in accordance with the Federal Rules.[228] But they had thirty days to install and operate malware on computers that visited the website.[229] The warrant application did not justify this extended time limit, nor did it indicate the source.

Three 2013 warrants in the District of Maryland, associated with the Freedom Hosting investigation, used the same formulation: fourteen days to begin

---

223. FED. R. CRIM. P. 41(e)(2)(A)(i).

224. Courts have, in the past, authorized deviations from Rule 41's time limit for subsequent forensic examination of seized computer data. *See* United States v. Kernell, No. 3:08-CR-142, 2010 U.S. Dist. LEXIS 32845, at *38-43 (E.D. Tenn. Mar. 31, 2010) (explaining the issue and collecting cases). That fact pattern is very different from government hacking, of course: police have long been authorized to inspect evidence after seizure. *See, e.g.*, United States v. Tillotson, No. 2:08-CR-33, 2008 U.S. Dist. LEXIS 120701, at *14 (E.D. Tenn. Nov. 13, 2008) ("The subsequent analysis of the computer's contents is not a search in the sense contemplated by Rule 41 . . . ."). And, at any rate, Rule 41 was explicitly amended to address the timing of post-seizure forensic examinations. FED. R. CRIM. P. 41(e)(2)(B) (clarifying that the Rule 41 time limits apply to "the seizure or on-site copying of the media or information, and not to any later off-site copying or review").

225. Third Amended Application for a Search Warrant, *supra* note 37, at 30.

226. *Id.* at 26.

227. *See* FED. R. CRIM. P. 41(e)(2)(A) ("The warrant must command the officer to execute the warrant within a specified time no longer than 14 days . . . ."); United States v. Grubbs, 547 U.S. 90, 95-96 (2006) (explaining that an anticipatory warrant involves a present determination by a judge).

228. *E.g.*, *Application for "Bulletin Board A" Search Warrant*, *supra* note 41, at 38.

229. *Id.* at 34.

the watering hole attack and thirty days to complete the attack.[230] The filings were virtually identical to the Operation Torpedo applications.

A 2013 warrant application in the Southern District of Texas requested a thirty-day period for installation and operation.[231] Once again, there was no asserted basis for the extended time limit. (In fact, the earlier Colorado affidavit expressly amended out a thirty-day time limit, explaining that it was "mistaken."[232])

Most recently, a 2015 warrant in the Eastern District of Virginia—the basis for Operation Pacifier—again parroted the earlier Operation Torpedo warrants. The FBI received approval to install their malware delivery on the seized website within fourteen days and to install and operate the malware on suspect computers within thirty days.[233] Again, there was no justification for the warrant's timing provisions.

Federal agents would, understandably, prefer not to be burdened with a malware warrant renewal every two weeks. Declassified FBI emails reflect extensive discussion about how to circumvent the explicit time limit imposed by the Fed-

230. Affidavit in Support of Application for a Search Warrant, *supra* note 42; Affidavit in Support of Application for Search Warrant, *In re* Search of Computs. that Access Target E-Mail Accounts, *supra* note 47; Affidavit in Support of Application for Search Warrant, *In re* Search of Computs. that Access the E-Mail Accounts Described in Attachment A, *supra* note 47.

231. *In re* Warrant To Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 756 (S.D. Tex. 2013) (malware warrant application seeking "prospective data obtained during a 30-day monitoring period").

232. Third Amended Application for a Search Warrant, *supra* note 37, at 7.

233. Affidavit in Support of Application for Search Warrant, *supra* note 43, at 30, 32-34.

eral Rules, including invocation of the (likely inapplicable) tracking device provisions of the Electronic Communications Privacy Act[234] and the (definitely inapplicable) All Writs Act.[235]

Rather than evade Rule 41 and its constitutional basis by invoking irrelevant statutes or slipping extra time into warrant applications, the government should propose a simple amendment. There is already a template: in order to facilitate location-tracking devices, the Federal Rules were amended in 2006 with provisions that set out discrete time periods for installation and operation.[236] A similar set of time limits should be expressly set out for government malware.

---

234. *See* Email from [Redacted] to [Redacted] Re: [Redacted] (Nov. 20, 2006), *in* 8 ELEC. FRONTIER FOUND., CIPAV FOIA RELEASE, *supra* note 167, at 154, 154 (discussing how to maximize the duration of malware operation under one court order). The tracking device statute, 18 U.S.C. § 3117 (2012), empowers courts to issue warrants for "tracking devices"; its implementation in Rule 41(e)(2)(C) specifies a maximum of ten days for installation and forty-five days for operation. The DOJ has consistently argued that these tracking device provisions do not cover purely electronic location-tracking techniques, in a bid to avoid a warrant requirement for mobile phone location tracking. *See, e.g.*, *In re* Application of the U.S. for an Order, 411 F. Supp. 2d 678, 681 (W.D. La. 2006). It would be incongruous for the DOJ to reverse that critical argument after a decade – and solely to extend a renewal clock in hacking cases. Moreover, identification malware does not itself locate a device in any conventional sense. Rather, it gives the government sufficient network and device configuration information to determine the owner's identity through follow-up investigation. And even if some of the functionality of government malware could be characterized as a tracking device, much of the functionality could not. Only a subset of the malware's operation would be covered by the longer time limit.

235. *See* Email from [Redacted] to [Redacted] Re: CIPAV Court Orders (Nov. 21, 2006), *in* 8 ELEC. FRONTIER FOUND., CIPAV FOIA RELEASE, *supra* note 167, at 149 ("One comment that has come in from my unit re the draft orders that should be forwarded to AUSA [redacted] is that he should also cite to the All Writs Act . . . ."). Courts invoke the All Writs Act, 28 U.S.C. § 1651, to compel third-party assistance with warrant execution. That includes assistance with ongoing electronic surveillance. *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 171-78 (1977) (sustaining the use of a warrant, in conjunction with the All Writs Act, to compel a telephone company to prospectively provide call records). But the All Writs Act is only relevant to third-party assistance associated with an electronic search, not any ongoing nature of the search. And even if there were any prospective search authority under the All Writs Act, it would be displaced by the more specific time limits imposed by Rule 41. *See* Pa. Bureau of Correction v. U.S. Marshals Serv., 474 U.S. 34, 40-43 (1985) (emphasizing that the All Writs Act is a "residual source of authority" that is overridden by more specific provisions).

236. FED. R. CRIM. P. 41(e)(2)(C) (setting out time limits for installation and operation of a location-tracking device pursuant to a warrant). Before federal and state rules were amended to address tracking devices, the ordinary law enforcement practice was to obtain a series of time-limited warrants (if they obtained warrants at all). *See, e.g.*, State v. Jackson, 76 P.3d 217, 220-21 (Wash. 2003) (describing a ten-day tracking device warrant, followed by a second ten-day warrant).

E. Notice

Since the Founding Era, courts have imposed notice requirements on law enforcement searches.[237] Ex ante notice, often dubbed "knock-and-announce," minimizes the disruption and damage associated with conducting a search.[238] The Supreme Court's most recent pre-execution notice guidance, in *Wilson v. Arkansas*, explained that ex ante notice is "an element of the reasonableness inquiry under the Fourth Amendment."[239]

Ex post notice serves different policy aims: it facilitates transparency and promotes confidence in government investigative practices that do not involve ex ante notice, ensuring that law enforcement officers comply with legal constraints.[240] While some courts have required after-the-fact notice based on the Fourth Amendment itself,[241] others only consider it a requirement of the Federal Rules of Criminal Procedure.[242]

Doctrine on ex ante notice clearly permits electronic surveillance without pre-execution announcement. A rule to the contrary would frustrate the very purpose of the investigation, tipping off suspects and preventing collection of evidence.[243] Wiretap super-warrants and location-tracking warrants are regularly issued with delayed notice, and Congress has provided general authority

---

237. *See* Jonathan Witmer-Rich, *The Rapid Rise of Delayed Notice Searches, and the Fourth Amendment "Rule Requiring Notice,"* 41 PEPP. L. REV. 509, 561-70 (2014) (reviewing an unbroken history of search notice requirements); *see also* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 802-03 (1994) (describing ex post notice as a central feature of Fourth Amendment warrants).

238. *See* Wilson v. Arkansas, 514 U.S. 927, 931-34 (1995) (explaining historical policy rationales for ex ante search notice).

239. *Id.* at 934.

240. *See generally* Brian L. Owsley, *To Unseal or Not To Unseal: The Judiciary's Role in Preventing Transparency in Electronic Surveillance Applications and Orders*, 5 CALIF. L. REV. CIR. 259 (2014) (discussing policy concerns associated with sealed surveillance orders).

241. *See, e.g.*, United States v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986) (holding that, if a court issues a warrant for surreptitious entry of a home, the Fourth Amendment mandates ex post notice with minimum delay); *see also* Berger v. New York, 388 U.S. 41, 60 (1967) (describing notice as a "requirement" for "conventional warrants").

242. *See, e.g.*, United States v. Pangburn, 983 F.2d 449, 449-50 (2d Cir. 1993) ("Although we have required that seven days notice be given after covert entries for which search without physical seizure has been authorized, that notice requirement is grounded in [Rule 41] and is not compelled by the Constitution.").

243. *See Berger*, 388 U.S. at 86 (Black, J., dissenting) (noting the futility of ex ante notice for wiretap surveillance, because it would undermine the government's ability to use such surveillance at all).

for delayed-notice ("sneak and peek") warrants.[244] The same procedure should be constitutionally permissible for government malware.

Ex post notice poses more difficult questions for law enforcement hacking. Is it required? Who receives the notice? How must it be provided? This Section establishes the principles for each of these subsidiary issues, then compares the resulting standards with current government practice.

Whether mandated by the Fourth Amendment or not, Rule 41 and its associated statutes are textually unambiguous. The government must *eventually* provide notice of a search warrant's execution.[245] Courts have broad, case-specific discretion to delay notice, but there must ultimately be notice. Hacking warrants, then, are subject to an ex post notice requirement too.

Conventional searches, wiretap super-warrants, and location-tracking warrants are all typically accompanied by eventual notice to the person with the privacy interest in the search. Courts have relaxed that requirement, under both the Fourth Amendment and Rule 41, where property or data are in the possession of a third-party business. For example, searches of parcels in transit have been held permissible with notice solely to the shipping company.[246] Searches of electronic content stored with a cloud service provider have similarly been allowed with notice only to the third-party business.[247] When executing a hacking warrant,

---

244. 18 U.S.C. § 2518(8)(d)(2012) (requiring actual service of notice within ninety days of a wiretap's conclusion); 18 U.S.C. § 3103a (2012) (granting general authority for delayed-notice search and seizure warrants); FED. R. CRIM. P. 41(f)(3) (permitting issuance of delayed-notice warrants where authorized by statute).

245. *See* Letter from William E. Moschella, Assistant Att'y Gen., to J. Dennis Hastert, Speaker, U.S. House of Representatives 7 (July 25, 2003), https://cdt.org/files/security/usapatriot/030725doj.pdf [http://perma.cc/XUE8-QS8K] (explaining that the delayed-notice search statute "requires law enforcement to give notice that a search warrant has been executed *in all circumstances*"); *cf. In re* Grand Jury Subpoena for [Redacted]@yahoo.com, No. 5:15-cr-90096-PSG, 2015 U.S. Dist. LEXIS 17379, at *1-2 (N.D. Cal. Feb. 5, 2015) (rejecting an indefinite gag order for electronic-data warrants and subpoenas).

246. *See, e.g.*, United States v. Zacher, 465 F.3d 336, 339 (8th Cir. 2006) (permitting notice of a package seizure by leaving a copy of the warrant with FedEx).

247. The Stored Communications Act (SCA) does not statutorily require notice to a subscriber after the government executes a search warrant for content stored with a service provider. 18 U.S.C. § 2703(b)(1)(A) (2012). Courts disagree on whether the SCA expressly eliminates any notice requirement, or merely defers to the notice provisions of Rule 41. *Compare* United States v. Scully, 108 F. Supp. 3d 59, 84-85 (E.D.N.Y. 2015) (concluding that the SCA mandates notice only where investigators have not obtained a warrant), *with In re* Application of the U.S. for an Order, 665 F. Supp. 2d 1210, 1216-21 (D. Or. 2009) (holding that the SCA incorporates Rule 41, including its notice provisions). Furthermore, at the time the SCA was enacted, Congress (and the courts) believed that content stored with a third-party business was often exempt from Fourth Amendment protection. *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (concluding that the SCA violates the Fourth Amendment by not

though, these third-party notice cases are not applicable, because the government is conducting a search of the suspect's *own* computer system by directly breaking into it. The notice associated with a hacking warrant, then, must be directed to the suspect herself.

The usual format for furnishing ex post notice of a search is actual notice – a copy of the warrant and a receipt for anything seized.[248] Wiretap super-warrants and location-tracking warrants follow the same approach.[249] The Fourth Amendment and Rule 41 do permit for constructive notice, though: investigators may leave a copy of the warrant and receipt at the location of the search, rather than handing it directly to the affected person.[250] Recent amendments to Rule 41

imposing a warrant requirement for content privately stored with third-party services). Based on a modern understanding, then, a warrant for content stored with a service provider must satisfy the notice requirements of the Fourth Amendment (to the extent they exist) and Rule 41 (to the extent they are not uniquely abrogated by the SCA). These notice requirements are both satisfied because the warrant is executed via a third party. *See In re* Application of the U.S. for an Order, 665 F. Supp. 2d at 1221-22 (holding that a warrant for stored content, executed via a third-party service provider, satisfies Rule 41's notice requirements); *id.* at 1222-24 (same for Fourth Amendment's notice requirement). Microsoft brought a Fourth Amendment challenge to the DOJ policy against notifying suspects whose stored content is searched. *See* Complaint for Declaratory Judgment, Microsoft Corp. v. U.S. Dep't of Justice at 13-14, No. 2:16-cv-00538-JLR (W.D. Wash. Apr. 14, 2016). Microsoft agreed to dismiss the case when the DOJ adopted a new policy on gag orders for service providers; the policy does not require notice to defendants. *See* Memorandum from Rod J. Rosenstein, Deputy Att'y Gen., to the Heads of the Dep't Law Enf't Components, the Heads of the Dep't Litigating Components, the Dir. of the Exec. Office for U.S. Att'ys, and All U.S. Att'ys (Oct. 19, 2017), https://assets.documentcloud.org/documents/4116081/Policy-Regarding-Applications-for-Protective.pdf [http://perma.cc/4X8C-5C4K].

248. FED. R. CRIM. P. 41(f)(1)(C) ("The officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken . . . .").

249. 18 U.S.C. § 2518(8)(d) (2012) ("[T]he issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory [of the wiretap application and execution]."); FED. R. CRIM. P. 41(f)(2)(C) ("[T]he officer executing a tracking-device warrant must serve a copy of the warrant on the person who was tracked or whose property was tracked. Service may be accomplished by delivering a copy to the person who, or whose property, was tracked . . . .").

250. FED. R. CRIM. P. 41(f)(1)(C) (allowing constructive notice by "leav[ing] a copy of the warrant and receipt at the place where the officer took the property"); *see also* FED. R. CRIM. P. 41(f)(2)(C) (allowing constructive notice of a tracking device warrant "by leaving a copy at the person's residence or usual place of abode with an individual of suitable age and discretion who resides at that location and by mailing a copy to the person's last known address").

clarify that the same minimum applies to a hacking warrant: government malware must be accompanied by constructive notice.[251]

In sum, Rule 41 and the Fourth Amendment impose three requirements for ex post notice of law enforcement hacking. First, the government must provide eventual notice. Second, the government must provide that notice to the device's owner. Third, the notice can be actual or constructive.

When the government executes a hacking warrant for a known computer, it appears to usually comply with these three requirements.[252] It provides eventual notice, to the computer's owner, through actual (not just constructive) service.

When the government deploys identification malware, by contrast, it presently falls far short of the three requirements. The current practice is to provide *no* notice of hacking to *any* affected person in *any* form until subsequent investigation discloses the identity of a hacked computer's likely owner. In more precise legal terms, the government believes it can particularly describe a computer to hack, but cannot reasonably describe a place to leave notice or a person to notify.

Recent hacking warrant applications almost uniformly rely upon this type of conditional ex post notice.[253] The operational consequence is that the government can hack with no transparency until it elects to subpoena a particular

---

251. FED. R. CRIM. P. 41(f)(1)(C) ("For a warrant to use remote access . . . the officer must make reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched . . . . Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person."). The amendment is a clarification of the existing notice requirement, rather than a new notice requirement. The rule text prior to the amendment still imposed a constructive notice requirement, and the delayed-notice statute still applied. *See* Memorandum from David Bitkower, *supra* note 92, at 8 (acknowledging that, even without the hacking-specific notice amendment to Rule 41, the DOJ is still bound by the delayed-notice statute when it deploys malware); *id.* at 9 (suggesting that the hacking-specific notice provision is grounded in the Fourth Amendment).

252. *See, e.g.*, United States v. Scarfo, 180 F. Supp. 2d 572, 574-75 (D.N.J. 2001) (providing a timeline for an FBI investigation). The author has confirmed this understanding with attorneys in the DOJ's Computer Crime and Intellectual Property Section.

253. *See, e.g.*, Third Amended Application for a Search Warrant, *supra* note 37, at 24 (specifying that "the government may delay providing a copy of the search warrant and the receipt for any property taken until the time that a suspect has been identified and has been placed in custody"); *id.* at 13 (requesting delayed notice "because the investigation has not identified an appropriate person to whom such notice can be given"); *Application for "Bulletin Board A" Search Warrant*, *supra* note 41, at 35-36 (specifying that "the government may delay providing a copy of the search warrant and the receipt for any property taken for thirty (30) days after a user of an 'activating' computer that accessed 'Bulletin Board A' has been identified to a sufficient degree as to provide notice"); Application and Affidavit for Search Warrant, *supra* note 4, at 16 (specifying that "the FBI may delay providing a copy of the search warrant and the receipt for any property taken until no more than thirty (30) days after such time as the name and location of the individual(s) using the activating computer is positively identified").

hacked user's ISP for subscriber information and identifies the user through further investigation.[254] That result poses an extraordinary privacy risk: the government can hack a large number of computers and then, in its exclusive discretion, furnish ex post notice to their owners.

This is, unfortunately, not a hypothetical. In the 2013 Freedom Hosting investigation, discussed above, the FBI deployed identification malware on seized webservers.[255] The FBI's watering hole strategy extended far beyond child pornography websites, reaching a number of non-criminal services – including a popular email provider.[256] Because of its approach to hacking warrant notice, though, the FBI appears to have been able to escape legal repercussions. Thousands of innocent American users (if not more) may have had their Fourth Amendment rights violated, and they may even have had meritorious claims for damages.[257] But they never learned that their computers were breached, because the FBI never subpoenaed for their identities.

The ideal resolution for hacking warrant notice would be another amendment to Rule 41. While the recent amendments did clarify that the government must make "reasonable efforts" to provide notice that is "reasonably calculated" to reach the person whose device was hacked,[258] the overall constructive notice requirement remains quite vague. Rule 41 already includes special notice procedures for tracking devices;[259] a similar set of provisions for government malware would lend much-needed clarity.

There are several possible strategies for constructive notice. The government might, for instance, change a hacked device's wallpaper or provide a pop-up alert. Another option would be to ensure actual notice by requiring the govern-

---

254. *See* United States v. Welch, 811 F.3d 275, 279-80 (8th Cir. 2016).

255. *See* Poulsen, *supra* note 42.

256. *See* Joseph Cox, *FBI May Have Hacked Innocent TorMail Users*, VICE: MOTHERBOARD (Jan. 21, 2016), http://motherboard.vice.com/en_us/article/wnx5px/fbi-may-have-hacked-innocent-tormail-users [http://perma.cc/UBV9-LAZ3]; Joseph Cox, *Unsealed Court Docs Show FBI Used Malware Like 'A Grenade'*, VICE: MOTHERBOARD (Nov. 7, 2016), http://motherboard.vice.com/en_us/article/wnxbqw/unsealed-court-docs-show-fbi-used-malware-like-a-grenade [http://perma.cc/SV3B-NSLM]; Poulsen, *supra* note 53; Kevin Poulsen, *If You Used This Secure Webmail Site, the FBI Has Your Inbox*, WIRED (Jan. 27, 2014), http://www.wired.com/2014/01/tormail/ [http://perma.cc/UY4T-EBFE].

257. *See* Joe Uchill, *ACLU Questions How Tor Email Users Got FBI-Deployed Malware*, HILL (Sept. 6, 2016), http://thehill.com/policy/cybersecurity/294618-aclu-why-did-email-service-users-get-fbi-deployed-malware [http://perma.cc/3D9M-N6LJ].

258. FED. R. CRIM. P. 41(f)(1)(C).

259. *See* FED. R. CRIM. P. 41(f)(2)(C) (describing special ex post notice provisions for tracking device warrants).

ment to subpoena a hacked device's ISP. Investigators could then guarantee actual notice through ordinary, in-person service. A compromise approach, which would minimize the marginal privacy impact for the device's owner while ensuring notice, would be to require the government to send a notification to a hacked device's ISP and compel the ISP to forward the notice to the relevant subscriber.[260] While all three approaches have drawbacks, it is difficult to maintain that *none* would satisfy the Rule 41 reasonableness standard.[261]

Regardless of whether Rule 41 is amended further, judges should cease issuing conditional-notice hacking warrants. As the Eighth Circuit recently recognized in a narrow ruling, the mandatory notice period for a malware search runs from the moment of search execution, not the moment that law enforcement agents learn a suspect's residential address or name.[262] The FBI's current practice is inconsistent with Rule 41 and (possibly) with the Fourth Amendment.

Judges should also insist that investigators write notice procedures into hacking warrant applications. Reasonable minds can disagree about the relative merits of the various approaches to constructive notice, but investigators should make a clear commitment to *some* approach in advance of installing malware.

F. Super-Warrant Requirements

In *Berger v. New York*, the Supreme Court indicated that the Fourth Amendment mandates more stringent procedures (dubbed "super-warrants" by some scholars) for interception of real-time communications.[263] As implemented in the Wiretap Act, the four core safeguards are: a determination that ordinary investigative techniques have failed or would likely be ineffective,[264] a particular

260. The FBI used a very similar notification process during a 2011 operation to disable the Coreflood botnet. *See* Gov't's Memorandum of Law in Support of Motion for a Temp. Restraining Order at *8, No. 3:11-cv-00561-VLB (D. Conn. Apr. 13, 2011).

261. The government might not want to leave malware resident on a suspect's computer longer than is necessary; subpoenaing a person's identity is an extra (albeit slight) privacy intrusion; and involving ISPs in sending notifications could introduce extra process burdens.

262. United States v. Welch, 811 F.3d 275, 279-81 (8th Cir. 2016).

263. 388 U.S. 41, 58-60 (1967).

264. 18 U.S.C. § 2518(1)(c) (2012).

description of the communications sought,[265] a firm time limit on the surveillance,[266] and a strategy for minimizing the interception of non-pertinent communications.[267] The Act permits wiretaps only for investigations into enumerated serious offenses,[268] and it requires prompt notice to the target.[269] The Wiretap Act also provides for annual reports on federal and state investigative practices.[270]

The *Berger* doctrine and the Wiretap Act plainly apply to phone wiretaps and audio bugs. If government malware activates a computer's microphone or otherwise intercepts a private spoken conversation, then it unambiguously must be operated with a super-warrant.[271]

In the decades following *Berger*, a number of cases posed the question of how the Fourth Amendment regulates video surveillance.[272] The unanimous conclusion among federal appellate courts has been that the Wiretap Act does not apply, but the *Berger* doctrine does. Courts must, consequently, borrow the core super-warrant protections from the Wiretap Act when authorizing video surveillance. The result for law enforcement malware is clear guidance: if agents seek to enable a computer's camera, they must obtain a super-warrant in advance.[273]

---

265. *Id.* § 2518(1)(b)(iii).

266. *Id.* § 2518(1)(d).

267. *Id.* § 2518(5).

268. *Id.* § 2518(3)(a).

269. *Id.* § 2518(8)(d).

270. *Id.* § 2519.

271. *See* Memorandum from David Bitkower to Judge Reena Raggi, *supra* note 92, at 9 (noting that the real-time communications content interception provisions of the Wiretap Act remain applicable to government hacking).

272. *See, e.g.*, United States v. Torres, 751 F.2d 875, 882-85 (7th Cir. 1984) (holding that the four core protections of the Wiretap Act are mandated by the Fourth Amendment for video surveillance and that the Federal Rules of Criminal Procedure are sufficiently flexible to accommodate those super-warrant safeguards); United States v. Biasucci, 786 F.2d 504, 507-12 (2d Cir. 1986) (following *Torres*); United States v. Cuevas-Sanchez, 821 F.2d 248, 251-52 (5th Cir. 1987) (adopting *Biasucci* and *Torres*); United States v. Mesa-Rincon, 911 F.2d 1433, 1436-46 (10th Cir. 1990) (applying the four core protections of the Wiretap Act to video surveillance); United States v. Koyomejian, 970 F.2d 536, 538-42 (9th Cir. 1992) (following *Cuevas-Sanchez*); United States v. Falls, 34 F.3d 674, 679-83 (8th Cir. 1994) (following and applying *Koyomejian*); United States v. Williams, 124 F.3d 411, 416-20 (3d Cir. 1997) (assuming the correctness of *Torres*).

273. *See In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 759-61 (S.D. Tex. 2013) (holding that the core *Berger* requirements apply to FBI malware that activates a computer's webcam).

In at least one malware-based investigation, though, the FBI failed to adhere to this requirement.[274]

Internet connectivity is a third easy-to-spot area of super-warrant coverage. Courts have consistently applied *Berger* and the Wiretap Act to real-time interception of online content.[275] If government malware intercepts content flowing through a computer's Wi-Fi, Bluetooth, Ethernet, or any other network interface, it must be installed and operated with a super-warrant.

A fourth fact pattern with unambiguous *Berger* and Wiretap Act coverage is where the government remotely monitors keystrokes or screen content in real-time or near-real-time.[276] When computer systems were only temporarily connected to the internet via a modem, the government was (arguably) able to evade heightened wiretapping requirements by recording only while the suspect was connected.[277] Given the modern reality of always-on internet connectivity, though, contemporaneous keystroke logging and screen capturing malware will generally require a super-warrant.

Outside of these four areas, the applicability of super-warrant doctrine to government hacking remains entirely unsettled. How should the courts and Congress more generally reconcile *Berger* and the Wiretap Act with government malware? The following Section proposes that government hacking should not just presumptively require a warrant—it should presumptively require a super-warrant.

---

274. *Id.*

275. *See, e.g.*, Joffe v. Google, Inc., 746 F.3d 920, 926-36 (9th Cir. 2013) (applying the Wiretap Act to wireless network interception); United States v. Councilman, 418 F.3d 67, 69-85 (1st Cir. 2005) (holding that email interception is covered under the Wiretap Act). If the government obtains solely real-time communications metadata in conjunction with a hack, it must comport with the pen register statute. 18 U.S.C. §§ 3121-3127 (2012). Since a warrant is substantively more rigorous then a pen/trap order, the only practical implication is that a federal investigation must be included in an annual Department of Justice pen/trap report. 18 U.S.C. § 3126 (2012).

276. *See* Luis v. Zang, No. 1:11-cv-884, 2013 WL 811816, at *4-9 (S.D. Ohio Mar. 5, 2013) (reviewing litigation on keyloggers and concluding that, if malware reports keystrokes to a remote party, it implicates the Wiretap Act); Shefts v. Petrakis, No. 10-cv-1104, 2012 U.S. Dist. LEXIS 130542, at *37-44 (C.D. Ill. Sept. 12, 2012) (holding that screen capture software that recorded email activity was covered by the Wiretap Act). Courts have generally not required that the transmission of recorded activity be precisely contemporaneous with the activity. *See* Williams v. Stoddard, No. PC 12-3664, 2015 R.I. Super. LEXIS 58, at *19-30 (R.I. Super. Ct. Feb. 11, 2015) (summarizing perspectives on wiretap timing).

277. *See* United States v. Scarfo, 180 F. Supp. 2d 572, 581-82 (D.N.J. 2001) (declining to apply the Wiretap Act to government malware that was configured to operate only when the computer's modem was active).

G. Policy Arguments in Favor of Always Requiring a Super-Warrant

In their concurring opinion in *Berger*, Justice Douglas and Justice Stewart highlighted their policy motivation for developing super-warrant doctrine. Electronic surveillance raises the specter of the "invisible policeman," they wrote.[278] "[I]t is the greatest of all invasions of privacy. It places a government agent in the bedroom, in the business conference, in the social hour, in the lawyer's office – everywhere and anywhere a 'bug' can be placed."[279]

These Justices surely could not have imagined modern information technology. Americans already carry around "minicomputers" in their pockets and on their wrists, replete with audio, video, and location sensors.[280] Government agents need not "place" any monitoring gear of their own; rather, they can subvert already-ubiquitous sensors and storage devices. If the potential for omnipresent state surveillance is the criterion for super-warrant doctrine, it is difficult to imagine a more qualifying investigative technique than government hacking.

Another rationale for imposing super-warrant requirements on law enforcement malware is the risk of dragnet data collection. Courts have emphasized that surreptitious audio and video surveillance tend to record innocent individuals and noncriminal conduct.[281] Law enforcement hacking poses dragnet risks, too, albeit in a somewhat different manner. Unlike with audio and video surveillance, the government can explicitly constrain the types of information that it receives. But, much like with audio and video recording, the government's investigative technique might affect the privacy interests of innocent (virtual) bystanders.

---

278. Berger v. New York, 388 U.S. 41, 65 (1967) (Douglas, J., concurring).

279. *Id.* at 64-65.

280. *See* Riley v. California, 134 S. Ct. 2473, 2489 (2014) ("The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

281. *See Berger*, 388 U.S. at 59 ("[T]he conversations of any and all persons coming into the area covered by the device will be seized indiscriminately and without regard to their connection with the crime under investigation."); *id.* at 65 (Douglas, J., concurring) ("The traditional wiretap or electronic eavesdropping device constitutes a dragnet, sweeping in all conversations within its scope – without regard to the participants or the nature of the conversations. It intrudes upon the privacy of those not even suspected of crime and intercepts the most intimate of conversations."); *see also* United States v. Biasucci, 786 F.2d 504, 510 (2d Cir. 1986) ("[C]oncern with the indiscriminate nature of electronic surveillance led the *Berger* Court to require that a warrant authorizing electronic surveillance be sufficiently precise so as to minimize the recording of activities not related to the crimes under investigation."); United States v. Torres, 751 F.2d 875, 885 (7th Cir. 1984) ("Television surveillance is identical *in its indiscriminate character* to wiretapping and bugging.").

And, because software scales so easily, the magnitude of collateral surveillance can be – and already may be – extraordinary. Under a super-warrant regime, investigators would have to be much more explicit about the scope of the devices they intend to hack and the information they seek to obtain.

A super-warrant mandate would also serve a beneficial channeling function. In many modern investigations, the government can obtain data through multiple means, such as by serving a warrant on a cloud service, physically seizing a suspect's computer, breaking into the suspect's cloud account, or hacking the suspect's computer. Warrants served on technology companies are preferable: they allow for regular transparency reporting, and they impose an added independent and impartial intermediary between the government and a wealth of user data.[282] Computer seizures are the next best option: they result in forensic analysis of a disk image, accompanied by a detailed log of investigative queries. Hacking techniques could circumvent these valuable transparency and review procedures, replacing them with ad hoc investigative practice. If the super-warrant doctrine applied, the government would have to explain why a cloud service or a seizure of a physical device would not work before a court sanctioned a hack.

Predictability is another virtue of a uniform super-warrant approach. The alternative would be carefully parsing the information that law enforcement obtains via hacking warrants, nitpicking which categories of data fall on which side of the super-warrant line. However difficult that approach may be today, it will only be more complex in the future. As more and more device functionality incorporates an online component – from applications to operating systems – courts would be left to arbitrarily delineate between warrant and super-warrant hacking.[283]

---

282. *See* Cardozo et al., *supra* note 74, at 13 (collecting business policies for handling government data demands, including annual transparency reports); Google, *Way of a Warrant*, YOUTUBE (Mar. 27, 2014), http://www.youtube.com/watch?v=MeKKHxcJfho [http://perma.cc/YS53-QUYA] (explaining that Google requires search warrants for user content, examines warrants for errors, narrows production for overbroad warrants, and notifies users of government demands); *see also, e.g.*, Opening Brief of Appellant Facebook, Inc. at 3-9, *In re* 381 Search Warrants Directed to Facebook, Inc. and Dated July 23, 2013, No. 30207-13 (N.Y. App. Div. June 20, 2014) (describing Facebook's challenge to search warrants from the New York County District Attorney for user content with questionable probable cause support and no date or content restrictions).

283. Imagine that the government hacks a user's device and monitors their files. So far, courts have concluded that super-warrant doctrine does not apply. But, in the future, a user's files will be automatically synced to remote services and other devices (e.g. Apple's iCloud). Those synced files are plainly electronic communications under the Wiretap Act and the *Berger* doctrine. Would the government then be required to obtain a super-warrant for file monitoring?

Externalities provide yet another reason for adopting super-warrants. In the wake of recent foreign intelligence disclosures, trust in information technology has become a critical commercial concern. Recent estimates place costs to American businesses in the tens of billions of dollars.[284] Trust in technology is also a critical civil liberties concern: researchers have documented speech chilling effects associated with government surveillance.[285] With each episode of hacking, the government imposes real costs that it does not internalize. A super-warrant requirement forces a degree of internalization, requiring extra detail and justification in the surveillance application.

Regardless of how courts respond to this normative argument, Congress could easily impose wiretap protections on law enforcement malware.[286] Legislation could simply combine the existing definition of hacking from the CFAA—messy as it is—with the existing super-warrant procedure from the Wiretap Act.[287]

---

284. *See* ED FERRERA ET AL., FORRESTER RESEARCH INC., GOVERNMENT SPYING WILL COST US VENDORS FEWER BILLIONS THAN INITIAL ESTIMATES 2 (2015) (estimating $47 billion in costs over three years); Daniel Castro & Alan McQuinn, *Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness*, INFO. TECH. & INNOVATION FOUND. 1 (June 2015), http://www2.itif.org/2015-beyond-usa-freedom-act.pdf [http://perma.cc/WX2U-SXCN] (estimating well over $35 billion in costs over three years).

285. *See, e.g.*, Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117-72 (2016) (concluding that surveillance disclosures chilled online activity); Alex Marthews & Catherine Tucker, Government Surveillance and Internet Search Behavior 40 (Mar. 15, 2017) (unpublished manuscript), http://ssrn.com/abstract=2412564 [http://perma.cc/BW5B-TY78] (finding that Google users' search behavior changed as a result of the surveillance revelations in June 2013); *see also* Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 RICH. L. REV. 465, 466-67 (2015) (linking government surveillance to First Amendment interests). *But see* Sören Preibusch, *Privacy Behaviors After Snowden*, 59 COMM. ACM 48, 48 (2015) (concluding that surveillance disclosures led to a decrease—not an increase—in privacy behaviors).

286. Whether privacy protections should be initially imposed by Congress or the courts is a subject of scholarly debate. *Compare* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 806 (2004) (arguing that Congress should be the primary source of privacy rules), *with* David Alan Sklansky, *Two More Ways Not To Think About Privacy and the Fourth Amendment*, 82 U. CHI. L. REV. 223, 224-33 (2015) (arguing that the courts should not wait for Congress to create privacy rules).

287. For example, Congress could amend the CFAA to read:

> (f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of an intelligence agency of the United States.
> (g) This section does not prohibit any lawfully authorized investigative or protective activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, provided that the agency has complied with the procedure established in 18 U.S.C. § 2518.

III. LESSONS FOR FOURTH AMENDMENT THEORY

Recent theoretical scholarship on the Fourth Amendment and electronic surveillance tends to be – at the risk of overgeneralization – either backward-looking or forward-looking. Some influential articles have carefully examined past judicial pronouncements in the interest of harmonizing seemingly inconsistent case law (and have often recommended that courts stay the course).[288] Other significant contributions have taken a normative tack, articulating how the principles of constitutional privacy protection could and should develop in the future.[289] Some of the best work has been process-oriented, examining the interbranch dynamics of surveillance regulation both descriptively and normatively.[290] When scholarly work has emphasized any particular technology,

288. *See, e.g.*, Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010) (arguing that Fourth Amendment protections for online communications generally track, and should continue to track, a content/noncontent distinction); Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011) [hereinafter Kerr, *An Equilibrium-Adjustment Theory*] (arguing that the evolution of Fourth Amendment law has balanced – and should continue to balance – changes in criminal and government technical capabilities); Kerr, *supra* note 31 (arguing that the evolution of Fourth Amendment law reflects four distinct conceptions of constitutional privacy); Kerr, *supra* note 29 (describing how constitutional privacy protections have applied and should continue to apply to transborder data flows).

289. *See, e.g.*, Baude & Stern, *supra* note 31 (recommending that Fourth Amendment law track statutory and common law privacy protections that apply to private actors); Daskal, *supra* note 29 (recommending that Fourth Amendment information privacy law abandon territoriality restrictions); Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199 (2009) (recommending that constitutional privacy protections track Lockean social contract theory and social norms); Nita A. Farahany, *Searching Secrets*, 160 U. PA. L. REV. 1239 (2012) (recommending using intellectual property law as a metaphor for Fourth Amendment protections); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309 (2012) (recommending a new balancing approach for Fourth Amendment protections); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101 (2008) (recommending reconceptualization of the Fourth Amendment as a right to security against state action); David Alan Sklansky, *Too Much Information: How Not To Think About Privacy and the Fourth Amendment*, 102 CAL. L. REV. 1069 (2014) (recommending reconceptualization of the Fourth Amendment as a protection for personal sovereignty); Solove, *supra* note 31 (recommending a new framework for Fourth Amendment law that emphasizes procedure over coverage).

290. *See, e.g.*, Orin S. Kerr, *The Effect of Legislation on Fourth Amendment Protection*, 115 MICH. L. REV. 1117 (2017) (reviewing judicial approaches to how congressional enactments influence Fourth Amendment articulation, and recommending that courts should independently interpret constitutional privacy protections); Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485 (2013) (noting tendencies in congressional surveillance regulation, and arguing that privacy protections should evolve from an interbranch dialogue);

it has tended to blast the application of old and lax doctrine as unwise and in need of course correction.[291]

Law enforcement hacking furnishes an opportunity for a new type of theoretical project on the application of the Fourth Amendment to electronic surveillance. The associated technologies are not pervasive and are not widely understood. In the courts, doctrinal puzzles are novel and unsolved; in the executive branch, prosecutors and agents are still hashing out their views; in Congress, legislators are just starting to take notice. In other words, the theoretical nexus for law enforcement hacking is not quite backward-looking or forward-looking—we are currently smack in the middle of the federal government's policy development process for electronic surveillance regulation.

This unique vantage point enables government malware to function as a natural experiment for testing Fourth Amendment hypotheses. Law enforcement hacking provides evidence—real, live, facts-on-the-ground evidence—about whether government practice aligns with scholarly approaches to the Fourth Amendment, and, if it does, what the consequences are.

This Part examines law enforcement hacking as a case study for three longstanding theoretical debates. First, what are the relative competencies of the three branches of the federal government when articulating electronic surveillance policy? Second, does Fourth Amendment doctrine seek to balance the capabilities of criminals and law enforcement, and should it? Third, how should common law and statutory privacy protections inform the scope of Fourth

---

John Rappaport, *Second-Order Regulation of Law Enforcement*, 103 CAL. L. REV. 205 (2015) (explaining how the Fourth Amendment can regulate policy, not just line-level police officers); Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039 (2016) (recommending implementation of administrative law strategies as a component of Fourth Amendment surveillance regulation).

291. *See, e.g.*, Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored Email*, 2008 U. CHI. LEGAL F. 121 (recommending against application of the third-party doctrine to stored email content); Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L.J. 946 (2016) (recommending constitutional privacy protection for location surveillance, based on reinvigoration of the Fourth Amendment's "effects" language); Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681 (2011) (recommending Fourth Amendment protection for cellphone location data); Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27 (2008) (recommending limits on the search incident to arrest doctrine as applied to electronic devices); Stephen E. Henderson, *Learning from All Fifty States: How To Apply the Fourth Amendment and Its State Analogs To Protect Third-Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373 (2006) (recommending limits on the third-party doctrine as applied to electronic surveillance); Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409 (2007) (recommending Fourth Amendment scrutiny for GPS-based location tracking).

Amendment safeguards? The following Sections respectively address these three areas of theoretical controversy.

A. *The Interbranch Dynamics of Surveillance Regulation*

1. *Competing Judicial and Scholarly Perspectives*

According to one strand of Fourth Amendment theory, the courts should not be the primary regulators of electronic surveillance. The leading judicial proponent is Judge Wilkinson of the Fourth Circuit, who has forcefully argued that Congress should be the lead branch for government privacy protection.[292] Writing for a unanimous panel in *In re Askin*, Judge Wilkinson concluded that federal agents had not effectuated a Fourth Amendment search when they intercepted a cordless telephone call because of a (since eliminated) Wiretap Act exception for cordless telephones.[293] Making decisions about surveillance policy, he reasoned, "demands a comprehension of complex technologies."[294] Congress has access to "the type of expertise that courts are . . . ill-equipped to acquire and to apply," so it should have the "primary job" of evaluating privacy impacts and updating the law.[295]

Judge Wilkinson recently refined his perspective in a concurring opinion in *United States v. Graham*, agreeing that investigators did not conduct a Fourth Amendment search when they obtained cell-site location information under the Stored Communications Act.[296] The touchstone of the Fourth Amendment is reasonableness, he emphasized, a term that is "literally crying out for balance between the competing interests of individual privacy and societal security."[297] Congress is the appropriate branch to strike that balance because of its greater access to expertise, greater ability to achieve legal consistency, and greater democratic legitimacy in making "high stakes and highly controversial" tradeoffs.[298]

Several Supreme Court Justices appear to have shared Judge Wilkinson's view—but with an important clarification. Writing in dissent in *Dalia v. United States*, Justice Stevens made the similar argument that surveillance legislation

292. *See* Kerr, *supra* note 290, at 1130-31 (tracing Judge Wilkinson's views); Sklansky, *supra* note 286, at 225-27 (similar).

293. 47 F.3d 100, 104-06 (4th Cir. 1995).

294. *Id.* at 106.

295. *Id.*

296. 824 F.3d 421, 438 (4th Cir. 2016) (Wilkinson, J., concurring).

297. *Id.* at 439.

298. *Id.* at 438-41.

should receive "special deference" from the courts because "Congress is better equipped than the Judiciary" to establish "a 'reasonable' accommodation" between privacy and law enforcement.[299] But that deference should apply only when Congress affirmatively authorizes a particular surveillance technique and establishes specific procedures for investigators.[300]

Justice Alito articulated a similar perspective in his concurrence in *Riley v. California*, writing that Congress and the state legislatures "are in a better position" than the courts to "respond to [technological] changes" and balance privacy and law enforcement.[301] He "would reconsider" his position if Congress responded by enacting a statute that specifically regulated mobile phone searches incident to arrest.[302]

The key theoretical divide between Judge Wilkinson and Justices Stevens and Alito is how they perceive the spectrum from congressional action to inaction. For Judge Wilkinson, *any* statute that establishes a procedure for a surveillance practice deserves great deference. In *Graham*, for instance, he deferred to a statute that was twenty years old and did not directly address the technology at issue. For Justices Stevens and Alito, by contrast, legislation only deserves constitutional deference if it speaks clearly about a specific surveillance technique in its modern context.

In a provocative 2004 article, Orin Kerr staked out a radical version of the prolegislature theory.[303] He argued that the courts should not only be reluctant to impose Fourth Amendment protections when Congress has acted, but also when Congress *has not* acted. Judicial privacy protections, Kerr argued in a subsequent article, risk "discourag[ing] legislative action by fostering a sense that the courts have occupied the field."[304] "The absence of judicial regulation invites legislative action."[305]

Several scholars have sharply criticized the prolegislature strand of Fourth Amendment theory and Kerr's version in particular. Dan Solove disputes that

---

299. 441 U.S. 238, 263-64 (1979) (Stevens, J., dissenting).

300. *Id.*

301. 134 S. Ct. 2473, 2497 (2014) (Alito, J., concurring).

302. *Id.*; *see also* United States v. Jones, 565 U.S. 400, 426-29 (2012) (Alito, J., concurring) (suggesting a similar point).

303. Kerr, *supra* note 286, at 806; *see also* Sklansky, *supra* note 286, at 226, 229-30 (explaining Kerr's argument).

304. Kerr, *supra* note 121, at 350.

305. *Id.* In recent work, Kerr appears to have significantly walked back this theory, arguing that judicial deference and inaction are only warranted to the extent that technology remains in flux; once technology has stabilized, courts should independently articulate surveillance regulation. *See* Kerr, *supra* note 290, at 1149-57.

Congress is inherently superior to the courts at crafting functional rules, keeping up with technological innovation, or understanding new technologies – in fact, he argues, the courts have been more successful at fashioning effective remedies and avoiding unprincipled gaps in coverage.[306] Courts may be slow and clumsy in reacting to new technology, but at least they do react – and they have effective tools for understanding new technologies (including experts and amici).[307]

David Sklansky has raised similar objections to the prolegislature theory.[308] Courts benefit from an adversarial process, he argues, with better representation for competing security and privacy interests (and less overrepresentation of law enforcement).[309] The process of case-by-case adjudication also provides an effective vehicle for legal reform as technology evolves.[310]

Erin Murphy has staked out a middle ground on the relative roles of the legislature and the judiciary in surveillance regulation. Based on a review of federal privacy statutes, Murphy concluded that congressional enactments are generally belated and piecemeal, excessively deferential to law enforcement interests, insufficiently protective of marginalized groups and the economically disadvantaged (who tend to disproportionately become criminal defendants), and limited in the safeguards and remedies that they provide.[311] The better approach to the Fourth Amendment, she argues, is an "interbranch dialogue" in which neither Congress nor the courts "assume sole or even primary responsibility for regulating privacy."[312]

The author's own view, tentatively, is most similar to Murphy's. In the author's contemporaneous experience as a legislative aide, there is almost no technical expertise on Capitol Hill, limited legal expertise on surveillance matters, disproportionate deference to the DOJ's assertions about law and policy, and pervasive drive to win support from law enforcement interest groups and appear "tough" on criminal justice issues. Lobbying by the DOJ and the Intelligence Community is frequent, sophisticated, and often at the member level. The executive branch is also exceptionally effective at leveraging its gatekeeping power over law enforcement and foreign intelligence information, inhibiting oversight

306. Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 761-74 (2005).

307. *Id.* at 771-73.

308. Sklansky, *supra* note 286, at 227-33.

309. *Id.* at 227; *see also* Peter P. Swire, Katz *Is Dead. Long Live* Katz, 102 MICH. L. REV. 904, 914-15 (2004) (arguing that the law enforcement community holds public choice advantages in congressional surveillance regulation).

310. Sklansky, *supra* note 286, at 227.

311. Murphy, *supra* note 290, at 495-525.

312. *Id.* at 537-38.

and creating a skewed perspective of policies and practices. Civil society groups that advocate for privacy protections are consistently inexperienced at lobbying, disorganized, off-message, and disconnected from decision makers. While the technology sector has previously participated in surveillance debates, it is increasingly distant from the topic owing to competing priorities.

Meanwhile, the author has had a number of opportunities to engage directly with the federal judiciary on surveillance matters, and has been consistently impressed by the intellectual curiosity and engagement of members of the bench. While the federal judiciary does lack technical expertise, it possesses unambiguous legal expertise, and its members exhibit a commitment to understanding novel law enforcement practices.

The author recognizes the democratic legitimacy of the legislative branch in articulating surveillance regulation and believes that Congress should play a more active role on the topic. But the author also believes that the judicial branch has its own unique legitimacy from its independence, sophistication, and counter-majoritarian record of protecting disfavored communities. The author's preference is an iterative process for developing surveillance law, leveraging the comparative advantages of each branch. A good template is wiretap doctrine, which emerged from an interplay between an executive branch commission, DOJ guidance, Supreme Court opinions, and a carefully crafted legislative framework.

Experience with law enforcement hacking will not resolve these weighty and longstanding theoretical debates about interbranch articulation of surveillance regulation. But it does offer several points of illumination for the scholarly discourse, presented in the following Sections.

2. *The Executive Branch Can Self-Regulate Privacy Practices Through Interagency Processes*

Fourth Amendment theory has tended to neglect the role of interagency policy development within the executive branch.[313] Articles and opinions that address interbranch dynamics tend to assume that the executive branch is synonymous with the law enforcement community and that investigative interests will consistently trample privacy considerations. In their view, we must rely on the

313. *See, e.g.*, Swire, *supra* note 309, at 914 ("The regulated industry of law enforcement has a concentrated interest in reducing regulation – pushing for fewer warrants, less onerous reporting requirements, and so on."). There are recent, noteworthy exceptions to this generalization. *See* Daphna Renan, *Pooling Powers*, 115 COLUM. L. REV. 211 (2015) (describing how federal agencies collaborate to enhance surveillance capabilities); Shirin Sinnar, *Protecting Rights from Within? Inspectors General and National Security Oversight*, 65 STAN. L. REV. 1027 (2013) (describing how inspectors general can constrain national security surveillance).

judiciary and the legislature to keep the zealous executive branch at bay. But experience with government malware shows that there is not always identity of interests among components of the executive branch. While the FBI was prepared to engage in law enforcement hacking without obtaining warrants, the Department of Justice, via its Computer Crime and Intellectual Property Section, was able to impose the Fourth Amendment's procedural safeguards.[314]

This phenomenon of interagency dialogue and oversight is not unique to malware. In the fall of 2015, the DOJ (note: not the FBI) imposed a requirement that cell-site simulators – devices used to track mobile phone location – only be operated pursuant to ordinary search warrants.[315] Just a month later, the Department of Homeland Security (note: not Immigration and Customs Enforcement, Customs and Border Protection, or the Secret Service) followed the DOJ's lead and implemented a nearly identical policy.[316]

These episodes of interagency surveillance constraints are, to be sure, exceptions to the norm. The executive branch unambiguously (and by design) seeks to vigorously investigate criminal activity with a powerful array of surveillance tools. But any account of the interbranch dynamics for Fourth Amendment protection must also acknowledge the powerful role of intra-branch dynamics and, especially, interagency policy development.[317]

3. *Executive Branch Privacy Protections Can Exceed Judicial and Legislative Protections*

As a corollary to the executive branch's ability to self-regulate through interagency processes, sometimes the executive branch adopts more privacy-protective procedures than are required by the courts or by Congress. In the context of

---

314. *See supra* notes 93-99 and accompanying text.

315. *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, U.S. DEP'T JUST. (Sept. 3, 2015), http://www.justice.gov/opa/file/767321/download [http://perma.cc/YTX2-YWSA]; *Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators*, U.S. DEP'T JUST. (Sept. 3, 2015), https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators [http://perma.cc/JXL9-LBRR].

316. Memorandum from Alejandro N. Mayorkas, Deputy Sec'y of Homeland Sec., to Component Chiefs, Department Policy Regarding the Use of Cell-Site Simulator Technology (Oct. 19, 2015), http://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf [http://perma.cc/R2C3-FEGU].

317. *Cf.* Renan, *supra* note 290, at 1115-23 (discussing options for intra-executive oversight of surveillance, with an emphasis on review for efficacy); Sinnar, *supra* note 313, at 1055-78 (discussing the role of agency inspectors general in protecting civil liberties during national security operations).

law enforcement hacking, FBI agents appear to have consistently applied for warrants to hack, and prosecutors have occasionally stipulated that hacking constitutes a Fourth Amendment search.[318] About half of lower courts have nevertheless responded by telling the executive branch that it need not go to the trouble: there is no search, and warrants are not necessary.[319] Congress, meanwhile, has declined to enact legislation in response.[320] This state of constitutional and statutory affairs may be temporary, as just one appellate court has reviewed whether the Fourth Amendment regulates law enforcement hacking, and Congress could still take action. At least for now, though, the executive branch is exceeding what some courts and Congress have required.

As with the phenomenon of executive branch self-regulation, it is important not to overstate this observation. Though it may be unusual for the executive branch to voluntarily exceed the bare minimum of surveillance procedure, it can happen, and it is an important consideration for Fourth Amendment theory that the judiciary and the legislature are not always the pro-privacy branches.

4. *Courts Exhibit Regulatory Capture in Law Enforcement Surveillance Litigation*

Another lesson from experience with government hacking is that the judiciary's independence from the law enforcement community is somewhat circumscribed. In the district courts in particular, federal prosecutors are consummate repeat players, and defendants in hacking cases tend to be unsympathetic.[321] The result appears to be a (mild) form of regulatory capture, in which prosecutorial arguments receive unusual deference. In the earliest district court opinions concluding that government malware is not a Fourth Amendment search, for example, the reasoning appears to be borrowed directly from prosecutorial briefing.[322]

---

318. *See supra* Section I.C.2.i.

319. *See supra* note 62 and accompanying text.

320. *See infra* Section III.A.6.

321. *See, e.g.*, United States v. Matish, 193 F. Supp. 3d 585, 621-22 (E.D. Va. 2016) ("The Court finds that due to the especially pernicious nature of child pornography and the continuing harm to the victims, the balance between any Tor user's alleged privacy interests and the Government's deployment of the NIT . . . weighs in favor of . . . [the] use of technology to counteract the measures taken by people who access child pornography online. The Government's efforts to contain child pornographers, terrorists and the like cannot remain frozen in time . . . ." (footnote omitted)).

322. *See, e.g.*, United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263, at *7 (W.D. Wash. Jan. 28, 2016) (accepting the government's position uncritically in three sentences); Government's Response to Second Motion to Suppress and Request for *Franks* Hearing at 17,

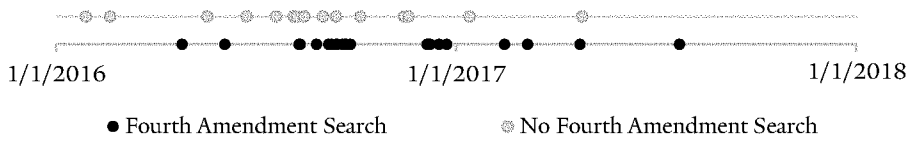
A number of commenters have observed that courts suffer from regulatory capture in the context of national security surveillance;[323] the same can occur in more routine criminal surveillance litigation.[324]

5. *Courts Are Capable of Understanding Novel Surveillance Technology*

Another takeaway for Fourth Amendment theory is that we need not be so concerned that the judiciary will be unable to understand modern technology.[325] To be sure, Tor is complex software and some opinions on law enforcement hacking do contain technical errors and oversights.[326] But, for the most part, the courts (or perhaps their clerks) have done a respectable job of understanding and explaining Tor and law enforcement hacking.[327]

FIGURE 2.

FEDERAL COURT OPINIONS ON WHETHER LAW ENFORCEMENT HACKING TO OBTAIN AN IP ADDRESS CONSTITUTES A FOURTH AMENDMENT SEARCH



Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263; United States' Response to Defendant's Motion to Suppress at 2, 6-7, *Michaud*, No. 3:15-cr-05351-RJB, 2016 WL 337263.

323. *See, e.g.*, Conor Clarke, *Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp?: Ex Parte Proceedings and the FISC Win Rate*, 66 STAN. L. REV. ONLINE 125 (2014) (engaging with claims that the Foreign Intelligence Surveillance Court exhibits regulatory capture).

324. *See, e.g.*, Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. REV. 589, 589-90 (2007) (describing how criminal surveillance law is often articulated in an ex parte posture, involving de facto deference to the Department of Justice's views).

325. *Cf.* Solove, *supra* note 306, at 771-73 (contesting the premise that legislatures are better equipped to deal with new technologies than judges).

326. *See, e.g.*, *Matish*, 193 F. Supp. 3d at 593-94 (asserting that Tor protects a user's IP address without any explanation of how it does so, which is essential for evaluating whether obtaining a Tor user's IP address constitutes a Fourth Amendment search); United States v. Werdene, 188 F. Supp. 3d 431, 444 (E.D. Pa. 2016) (claiming wrongly that the defendant's "IP address was subsequently bounced from node to node within the Tor network").

327. *See, e.g.*, United States v. Eure, No. 2:16-cr-43, 2016 WL 4059663, at *1-4 (E.D. Va. July 28, 2016); United States v. Darby, 190 F. Supp. 3d 520, 524-27 (E.D. Va. 2016); United States v. Arterbury, No. 15-CR-182-JHP, 2016 BL 133752, at *1-3 (N.D. Okla. Apr. 25, 2016).

Figure 2 traces the issuance of federal opinions on whether hacking is a search. It illustrates that early opinions on this issue, in the first half of 2016, tended to hold that hacking was not necessarily a search; the more recent opinions have reached the opposite – and, as this Article argues, correct – conclusion.

A review of the underlying opinions suggests that the reason for the mid-2016 inversion is that district courts learned from each other. Not coincidentally, the early district court opinions that offered the best technical explanation of Tor and government malware tended to conclude that law enforcement hacking is a Fourth Amendment search.[328] The longitudinal process of case-by-case articulation allowed those courts to act as thought leaders, such that subsequent opinions could build upon their factual explanation and legal analysis.[329] Thus, while each individual court might not be particularly technically sophisticated, in the aggregate and over time, the district courts are converging on accurate facts and sound law.

This phenomenon suggests a broader lesson for Fourth Amendment theory and judicial sophistication about novel surveillance technologies. When the law enforcement community deploys a new surveillance capability in a manner that will be litigated with frequency in myriad venues, there is less cause for concern (at least in the long run) about the judiciary's familiarity with new technology. When a law enforcement agency deploys a one-off, bespoke surveillance technology, by contrast, courts will not benefit from each other's wisdom. In these cases, litigants and judges will need to be more attuned to seeking technical input and engaging with technical details.

6. *Congress Is Not Taking Action*

Perhaps the most important lesson for interbranch development of surveillance regulation is that Congress has done nothing to respond to law enforcement hacking. There is no legislation – neither introduced nor in draft form – that would establish procedural guardrails for government malware. The sole effort at legislative action, championed by Senator Ron Wyden, is a bill that would prevent the government from conducting watering hole attacks.[330] Despite vocal opposition to the practice – with Google and a range of civil society

328. *E.g.*, United States v. Anzalone, 208 F. Supp. 3d 358, 360-61, 363-64 (D. Mass. 2016) (explaining both Tor and the government's malware); *Arterbury*, 2016 BL 133752, at *1-2 (similar).

329. *E.g.*, United States v. Workman, 863 F.3d 1313, 1315-16 (10th Cir. 2017) (providing an explanation and an essentially accurate step-by-step diagram of law enforcement hacking).

330. Stopping Mass Hacking Act, S. 2952, 114th Cong. (2016); *see also* Stopping Mass Hacking Act, H.R. 5321, 114th Cong. (2016) (proposing identical language in the House of Representatives).

groups registering their protests[331] – Senator Wyden's bill has only mustered five cosponsors in the Senate and six in the House of Representatives.[332]

Whatever the abstract merits of congressional primacy in surveillance regulation, the reality is that Congress is not currently in the business of regulating surveillance. As long as that remains the case – whatever the institutional limits of the judiciary and however much it should defer to affirmative legislative enactments – the courts must remain the primary check and balance for electronic surveillance.

B. Equilibrium-Adjustment and Substitution Theories Are Indeterminate and Risk Misleading Courts

In a separate strand of Fourth Amendment theory, scholars have wrestled with how to substantively reconcile evolving technology and established law. One prominent approach, occasionally invoked by the judiciary and recently formalized by Orin Kerr, attempts to preserve the balance between criminal and law enforcement technical capabilities. In a 2009 article, Kerr argued that the Fourth Amendment should not protect technologies that create "substitution" effects by enabling criminals to remove their activity from unprotected public spaces.[333] In a 2011 sequel, Kerr refined and generalized the equilibrium-adjustment theory, arguing that Fourth Amendment safeguards should be calibrated to perpetuate an established balance between privacy and policing.[334]

Academic reactions to Kerr's theory have been mixed. In perhaps the most comprehensive response, Paul Ohm argues that equilibrium adjustment is a helpful intellectual framework for exploring Fourth Amendment dilemmas, but has no normative force of its own.[335] Recognizing the existence of a balance sheet, Ohm explains, does not inform what should go into each column – nor does it explain how to tally up and compare the columns.[336]

---

331. *See, e.g.*, Richard Salgado, *A Small Rule Change that Could Give the U.S. Government Sweeping New Warrant Power*, GOOGLE PUB. POL'Y BLOG (Feb. 18, 2015), http://publicpolicy.google-blog.com/2015/02/a-small-rule-change-that-could-give-us.html [http://perma.cc/PSB4-UBVY].

332. *Cosponsors: H.R.1110 – 115th Congress (2017-2018)*, CONGRESS.GOV, http://www.congress.gov/bill/115th-congress/house-bill/1110/cosponsors [http://perma.cc/4RZP-T4RX]; *Cosponsors: S.406 – 115th Congress (2017-2018)*, CONGRESS.GOV, http://www.congress.gov/bill/115th-congress/senate-bill/406/cosponsors [http://perma.cc/KD2K-6GYL].

333. Kerr, *supra* note 147, at 573-81.

334. Kerr, *An Equilibrium-Adjustment Theory*, *supra* note 288.

335. Ohm, *supra* note 289, at 1339-47.

336. *Id.* at 1344.

David Sklansky has raised similar concerns.[337] The process of equilibrium adjustment, Sklansky observes, requires selecting a target balance of privacy and law enforcement. But the process of selecting a reference point requires an underlying policy judgment.[338] What's more, privacy protection and law enforcement power have myriad and unquantifiable dimensions.[339] Even if there were a reference point, any measurement comparing against the reference point would be laden with additional policy judgments.

The present wave of litigation addressing government malware provides a case study in the feasibility and consequences of equilibrium adjustment. The experience lends substantial support to the criticisms advanced by Ohm and Sklansky and suggests that equilibrium adjustment is not just indeterminate, but also prone to leading courts astray.

Beginning with the indeterminacy problem, articulating a definitive equilibrium-adjustment narrative for law enforcement hacking is an impossible task. First, what is the appropriate reference point for calibrating the policing and privacy interests associated with government hacking?[340] Is it 1791, when the Fourth Amendment was ratified? Is it 1876, when Alexander Graham Bell received a patent for the telephone? What about 1968, when researcher Douglas Engelbart gave the "mother of all demos" that foreshadowed modern personal computers? How about 1990, when Tim Berners-Lee developed the web? Equilibrium adjustment is, essentially, a type of techno-originalism—but without a distinct constitutional moment to serve as a point of reference.

Moreover, even if there were a definitive reference point, calculating the equilibrium adjustment for law enforcement hacking would still be hopelessly indeterminate. On the law enforcement side of the ledger, criminals use Tor to mask their illicit online activity and use encryption to frustrate access to communications and stored data. In the civil liberties column, government malware is difficult for courts to supervise, easily mistargeted, and rife with risk for negative social costs.[341] From a broader societal perspective, Tor provides legitimate and

---

337. Sklansky, *supra* note 286, at 233-41.

338. *See id.* at 236-37.

339. *Id.* at 237-38.

340. *Id.* at 236 & n.90.

341. *See, e.g.*, Azam Ahmed & Nicole Perlroth, *Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families*, N.Y. TIMES (June 19, 2017), http://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html [http://perma.cc/2L5K-57FF] (reporting how elements of the Mexican government appear to have targeted journalists with malware). *See generally supra* Section II.G (discussing risks and negative externalities associated with law enforcement hacking).

valuable functionality, such as enabling internet access and anonymity for dissidents living under repressive regimes,[342] and encryption is a critical safeguard against online crime and data breach.[343] The theory of equilibrium adjustment requires that we measure up and balance these policing, privacy, and societal considerations in comparison to a reference point. But how? Any answer must necessarily resort to an extrinsic normative framework.

The indeterminacy that Ohm and Sklansky identify is not the only shortcoming of the equilibrium-adjustment approach. Lower court experience with law enforcement hacking highlights an additional, practical danger associated with the equilibrium-adjustment theory. In reaching the conclusion that government malware is not necessarily a Fourth Amendment search, courts have explained their reasoning in various ways: a defendant "should not be *rewarded* for allegedly obtaining contraband through his virtual travel through interstate and foreign commerce on a Tor hidden service,"[344] should not "*serendipitously* receive Fourth Amendment protection because he used Tor in an effort to evade detection,"[345] and "cannot *conceal* his deviant behavior through Internet tricks."[346]

These opinions reflect a specific version of equilibrium adjustment. The reference point is that, prior to adoption of anonymizing technology, law enforcement investigators could obtain a suspect's IP address without a search warrant. The deviation from that reference point is that criminals have an enhanced technical capability (anonymizing software) that frustrates conventional investigative techniques. As a counterbalance, novel law enforcement measures (hacking) that circumvent the new criminal capability should not be subject to heightened procedural requirements.

This type of myopic equilibrium adjustment focuses on just one side of the ledger—the enhanced capabilities that technology affords to criminals—and adopts as its reference point the time immediately preceding introduction of the new technology. Courts then adjust the equilibrium so that in the period following the introduction of the new technology, the government can continue accessing the same classes of investigative data with the same legal procedures.

---

342. *Users of Tor*, TOR, http://www.torproject.org/about/torusers.html.en [http://perma.cc/85TF-Q266].

343. *See* H. COMM. ON THE JUDICIARY, 114TH CONG., ENCRYPTION WORKING GROUP YEAR-END REP. (2016), http://judiciary.house.gov/wp-content/uploads/2016/12/20161220EWGFINAL Report.pdf [http://perma.cc/67JE-WBT3].

344. United States v. Matish, 193 F. Supp. 3d 585, 621 (E.D. Va. 2016) (emphasis added).

345. United States v. Werdene, 188 F. Supp. 3d 431, 446 (E.D. Pa. 2016) (emphasis added) (internal quotation mark omitted).

346. United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *6 (C.D. Cal. Aug. 8, 2016) (emphasis added).

If this recurrent reasoning is representative, judicial adoption of equilibrium adjustment risks a "ratchet-up effect" for warrantless surveillance capabilities.[347] For each new technology that criminals adopt to conceal evidence, law enforcement can deploy a novel investigative technique that circumvents the criminal technology without being subject to heightened procedural protections.[348] Equilibrium adjustment would turn the conventional Fourth Amendment analysis on its head. Typically, the more an individual takes measures to protect his or her privacy, the more he or she should be entitled to constitutional privacy protections.[349] Equilibrium adjustment risks leading courts to the opposite conclusion, perversely finding that privacy measures justify additional intrusions.

C. *Positive Law Is a Factual Guide, but Not Necessarily a Legal Guide, for Constitutional Articulation*

A third strand of Fourth Amendment theory examines the proper relationship between the privacy protections that regulate private actors (by statute or common law) and the privacy protections that regulate law enforcement agents (under the Fourth Amendment). Recent scholarship has explored a range of alternatives: protections against private actors may be completely independent from constitutional protections, they may inform constitutional doctrine, they may set a minimum for constitutional safeguards, or they may replace Fourth Amendment law outright.[350]

---

347. *Cf.* Swire, *supra* note 309, at 914 (describing a "ratchet-up effect" in legislative surveillance authorities, because law enforcement agencies can persuasively lobby for lesser protections).

348. *See id.*

349. *See, e.g.*, United States v. Kahler, No. 16-cr-20551, 2017 WL 586707, at *7 (E.D. Mich. Feb. 14, 2017) ("The Government argues that, despite using a software which exists only to veil the user's IP address from prying eyes, the user has no reasonable privacy interest in his or her IP address. This argument has little to recommend it. If a user who has taken special precautions to hide his IP address does not suffer a Fourth Amendment violation when a law enforcement officer compels his computer to disclose the IP address . . . then it is difficult to imagine *any* kind of online activity which is protected by the Fourth Amendment.").

350. *See, e.g.*, Baude & Stern, *supra* note 31, at 1888-89 (proposing that Fourth Amendment regulation of privacy track statutory and common-law regulations of privacy); Kerr, *supra* note 290 (describing possible relationships between statutory privacy regulation – much of which restricts both private and government intrusions – and Fourth Amendment privacy regulation); Richard M. Re, *The Positive Law Floor*, 129 HARV. L. REV. F. 313 (2016) (proposing that statutory and common-law regulations of privacy set a minimum for Fourth Amendment protections).

The legal response to government malware highlights two noteworthy elements of the relationship between positive law and Fourth Amendment protection. First, regulation of private actors can furnish a valuable analytical framework for puzzling through fact patterns involving government actors. The CFAA, the primary federal computer crime statute, expressly does not apply to law enforcement activities.[351] But the way in which the CFAA dissects computer trespass – analyzing security and privacy interests both in computer systems and in the data that they store – constitutes a signpost for Fourth Amendment evaluation.[352] The analysis in Part I, for example, was inspired by the CFAA's protections for both devices and data. Thus, regardless of whether positive law *substantively* shapes or replaces constitutional privacy doctrine, positive law has an important role in *framing* fact patterns for constitutional analysis.

The connection between the CFAA and the Fourth Amendment also highlights why positive law alone cannot satisfactorily scope constitutional privacy protections. Under current CFAA doctrine, a website operator can establish liability by sending a cease-and-desist letter to a would-be defendant; any further website access by the defendant is actionable as computer trespass.[353] But imagine the result if the same standard scoped Fourth Amendment protection. If the operator of a criminal website sent a cease-and-desist letter to the director of the FBI, would federal agents then need to obtain a warrant to access the website? The hypothetical is an absurdity, of course, and contrary to current doctrine: law enforcement agents are permitted to enter any areas that are reasonably open to the public.[354] But it highlights that positive law can sometimes be *too* protective of privacy to function as a plausible Fourth Amendment stand-in.

---

351. Computer Fraud and Abuse Act § 2(h), 18 U.S.C. § 1030(f) (2012).

352. *See* Mayer, *supra* note 159, at 1663-64 (describing how the CFAA protects both devices and data).

353. *See* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1065-69 (9th Cir. 2016) (allowing a CFAA claim where the plaintiff expressly and completely revoked defendant's authorization by letter); Craigslist Inc. v. 3Taps Inc., 964 F. Supp. 2d 1178, 1181-84 (N.D. Cal. 2013) (same); Weingand v. Harland Fin. Solutions, Inc., No. C-11-3109 EMC, 2012 WL 2327660, at *3 (N.D. Cal. June 19, 2012) (allowing a CFAA claim where the plaintiff arguably delineated the defendant's authorization by verbal statement); Mayer, *supra* note 159, at 1654-56 (describing "without authorization" liability under CFAA).

354. *See, e.g.*, Oliver v. United States, 466 U.S. 170, 177 (1984) (holding that "the government's intrusion upon the open fields is not one of those 'unreasonable searches' proscribed by the texts of the Fourth Amendment").

CONCLUSION

The government's track record with law enforcement hacking is hardly stellar. Descriptions of malware are often ambiguous and euphemistic.[355] The government has strained the Fourth Amendment, asserting that no warrant is required at all (Part I), or that a warrant is only required for a moment (Section II.A). Agents have botched probable cause and particularity, possibly leading to hacks of innocent users (Section II.B). Warrant applications have ignored venue restrictions established by statute and rule (Section II.C), as well as the unambiguous time limits of Rule 41 (Section II.D). Almost every unsealed warrant for identification malware relies upon conditional notice, in violation of Rule 41 and (possibly) the Fourth Amendment (Section II.E). And, finally, the government has not properly applied for super-warrants in scenarios where they are required (Section II.F). This string of procedural defects should weigh heavily in favor of heightened judicial scrutiny, such as an across-the-board super-warrant requirement (Section II.G).

In the years to come, government hacking will only become more common. Law enforcement agencies have expressed their alarm about the increasing pervasiveness of device and communications encryption, which frustrates conventional electronic surveillance techniques.[356] Malware is one of the few technical countermeasures available to the government.

Law enforcement agencies should be able to hack. It can be a legitimate and effective investigative technique. There is nothing inherently wrong with the

---

355. *See In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753 (S.D. Tex. 2013) (denying and criticizing a malware warrant application); Stanford Ctr. for Internet & Soc'y, *In Conversation: The Hon. Stephen W. Smith and Former Magistrate Judge Paul S. Grewal*, YOUTUBE (Nov. 9, 2016), https://www.youtube.com/watch?v=3-fycsuHXpU [http://perma.cc/SBX4-U43A] (explaining that "many judges . . . don't exactly know what they are being presented with" and applications can include "a very anodyne term like 'network investigative technique'").

356. *See* James B. Comey, *Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy*, FED. BUREAU INVESTIGATION (July 8, 2015), https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy [http://perma.cc/K4FQ-B7VX] ("[E]ncryption as currently implemented poses real barriers to law enforcement's ability to seek information . . . ."); Sally Quillian Yates, *Deputy Attorney General Sally Quillian Yates Delivers Oral Testimony Before the Senate Judiciary Committee*, U.S. DEP'T JUST. (July 8, 2015), http://www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-oral-testimony-senate-judiciary [http://perma.cc/32QD-GAYV] ("[E]ncryption has been designed so that the information is only available to the user and the providers are unable to comply with the court order or warrant.").

government compromising computer systems. But appropriate procedural protections are vital, and present practices leave much room for improvement.

APPENDIX

Cases concluding that the Fourth Amendment regulates government hacking to discover a device's IP address
United States v. Horton, 863 F.3d 1041, 1047 (8th Cir. 2017)
United States v. Wheeler, No. 1:15-cr-00390-MHC-JFK, slip op. at 11-14 (N.D. Ga. June 12, 2017)
United States v. Taylor, No. 2:16-cr-00203-KOB-JEO-1, 2017 WL 1437511, at *8 (N.D. Ala. Apr. 24, 2017)
United States v. Hachey, No. 5:16-cr-00128-JLS, at *16 (E.D. Pa. Mar. 7, 2017)
United States v. Kahler, 236 F. Supp. 3d. 1009, 1013 (E.D. Mich. 2017)
United States v. Dzwonczyk, No. 4:15-CR-3134, 2016 WL 7428390, at *11 (D. Neb. Dec. 23, 2016)
United States v. Vortman, No. 16-cr-00210-TEH-1, 2016 WL 7324987, at *7 (N.D. Cal. Dec. 16, 2016)
United States v. Hammond, No. 16-cr-00102-JD-1, 2016 WL 7157762, at *2 (N.D. Cal. Dec. 8, 2016)
United States v. Duncan, No. 3:15-cr-00414-JO, 2016 WL 7131475, at *2 (D. Or. Dec. 6, 2016)
United States v. Owens, No. 16-CR-38-JPS, 2016 WL 7053195, at *5 (E.D. Wis. Dec. 5, 2016)
United States v. Allain, 213 F. Supp. 3d 236, 245 n.5 (D. Mass. 2016)
United States v. Anzalone, 208 F. Supp. 3d 358, 366 (D. Mass. 2016)
United States v. Broy, 209 F. Supp. 3d 1045, 1055 (C.D. Ill. 2016)
United States v. Croghan, 209 F. Supp. 3d 1080, 1092 (S.D. Iowa 2016), *rev'd on other grounds sub nom*. United States v. Horton, 863 F.3d 1041 (8th Cir. 2017)
United States v. Ammons, 207 F. Supp. 3d 732, 739 (W.D. Ky. 2016)
United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223, at *3 (W.D. Tex. Sept. 9, 2016)
United States v. Workman, 205 F. Supp. 3d 1256, 1265 (D. Colo. 2016), *rev'd on other grounds*, 863 F.3d 1313 (10th Cir. 2017)
United States v. Scarbrough, No. 3:16-cr-00035, 2016 WL 8677187, at *6 (E.D. Tenn. Aug. 26, 2016) (report and recommendation)
United States v. Adams, No. 6:16-cr-11-Orl-40GJK, 2016 WL 4212079, at *4 (M.D. Fla. Aug. 10, 2016)
United States v. Darby, 190 F. Supp. 3d 520, 530 (E.D. Va. 2016)
United States v. Arterbury, No. 15-CR-182-JHP, 2016 BL 133752, at *13 (N.D. Okla. Apr. 25, 2016)

Cases concluding that the Fourth Amendment does not regulate this form of government hacking
United States v. Halgren, No. SA-16-CR-008-XR, 2017 WL 3741558, at *3 (W.D. Tex. Aug. 30, 2017)
United States v. Scanlon, No. 2:16-cr-00073-cr, slip op. at 18-19 (D. Vt. Apr. 26, 2017)
United States v. Bee, No. 16-00002-01-CR-W-GAF, 2017 WL 424905, at *6 (W.D. Mo. Jan. 13, 2017) (report and recommendation)
United States v. Lough, 221 F. Supp. 3d 770, 775 (N.D.W. Va. Nov. 18 2016)
United States v. Kienast, No. 16-CR-103, 2016 WL 6683481, at *4 (E.D. Wis. Nov. 14, 2016)
United States v. Dzwonczyk, No. 4:15CR3134, slip op. at 8 (D. Neb. Oct. 5, 2016) (findings, recommendation, and order)
United States v. Jean, 207 F. Supp. 3d 920, 933 (W.D. Ark. 2016)
United States v. Henderson, No. 5:15-cr-00565-WHO-1, 2016 WL 4549108, at *5 (N.D. Cal. Sept. 1, 2016)
United States v. Johnson, No. 15-00340-01-CR-W-GAF, slip op. at 9 (W.D. Mo. Aug. 16, 2016) (report and recommendation)
United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *4 (C.D. Cal. Aug. 8, 2016)
United States v. Laurita, No. 8:13CR107, 2016 WL 4179365, at *5 (D. Neb. Aug. 5, 2016)
United States v. Rivera, No. 2:15-cr-00266-CJB-KWR, at *19 (E.D. La. July 20, 2016)
United States v. Matish, 193 F. Supp. 3d 585, 608 (E.D. Va. 2016)
United States v. Werdene, 188 F. Supp. 3d 431, 446 (E.D. Pa. 2016)
United States v. Stamper, No. 1:15cr109, 2016 WL 695660, at *3 (S.D. Ohio Feb. 19, 2016)
United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263, at *8 (W.D. Wash. Jan. 28, 2016)